



PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO

NÚMERO DO PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016
NÚMERO DO PROCESSO E MODALIDADE	Pregão Eletrônico n.º 001/2023
EXERCÍCIO FINANCEIRO	2023
SETOR SOLICITANTE	Gerência de Tecnologia da Informação
OBJETO DA LICITAÇÃO	Contratação de empresa especializada em SERVIÇOS GERENCIADOS DE SEGURANÇA.
DATA DE INÍCIO DO PROCESSO	18/01/2023

PE-002/AF
11/8/2021

FORMALIZAÇÃO DA DEMANDA

Sector Requisitante: Gerência de Tecnologia da Informação - Getin	
Responsável pela Demanda: Cláudio Mário Araújo da Silva	Matrícula: 359
Data do Pedido	15/12/2022

Necessidade da Contratação

1. Monitorar a utilização dos recursos e sistemas críticos, sob o aspecto de Segurança da Informação.
2. Tratar adequadamente os incidentes de Segurança da Informação;
3. Reduzir as vulnerabilidades de Segurança da Informação do ambiente do CRCMG;

Justificativa da necessidade da contratação considerando o Planejamento Estratégico, se for o caso.

Em decorrência dos constantes ataques cibernéticos a diversas instituições públicas e privadas e da implantação da LGPD no CRCMG, que exige a adoção de medidas de segurança, torna-se indispensável a aplicação de boas práticas de segurança da informação no ambiente tecnológico do CRCMG.

Diante do crescimento exponencial de ameaças e ataques sofridos a empresas privadas e órgãos públicos no Brasil e no mundo, investimentos contínuos em segurança da informação são fundamentais para a mitigação de riscos de segurança associados ao negócio de maneira a resguardar a confidencialidade, a disponibilidade e a integridade das informações.

O cenário de ameaças à segurança da informação não se resume a ataques aos serviços de TI pela Internet. Tentativas de acesso não autorizadas, infecção por arquivos maliciosos (vírus), e-mails indesejados (SPAMs), engenharia social, entre outros, são exemplos de eventos que podem apresentar riscos à segurança de TI. Até mesmo colaboradores não conscientes ou mal-intencionados representam risco potencial à segurança da informação.

O Conselho Regional de Contabilidade de Minas Gerais vem utilizando, cada vez mais, soluções de TI na busca de aperfeiçoamento da sua missão institucional e gestão pública. Junto a isso, vem também disponibilizando aos seus colaboradores, aos profissionais contábeis e à sociedade diversos serviços de TI. Nesse cenário, diversas foram as mudanças: tanto em termos de quantidade de serviços oferecidos quanto a diversidade de soluções. Conforme cresce a oferta de serviços aumentam-se os riscos relacionados e a necessidade de monitoramento.

Nesse sentido, incidentes de segurança da informação, como nas hipóteses de violação, roubo ou perda de informações custodiadas pelo CRCMG, podem constituir possíveis situações capazes de inviabilizar, senão a totalidade, parte das atividades desta entidade. Assim, a ocorrência de eventuais sinistros poderia provocar o vazamento de informações, prejuízo à sua imagem, podendo ainda a entidade que responder pelos danos causados.

Como o CRCMG não dispõe de funcionários em seu quadro de empregados nem cargo em seu plano de cargos e salários para atender à demanda com elevado nível de conhecimento que o ambiente exige, considera-se necessária a contratação de empresa especializada para esta finalidade, que forneça pessoal especializado em segurança da informação que propicie a integridade, a confidencialidade, a autenticidade e a disponibilidade dos dados, através de um monitoramento preventivo e contínuo de segurança da informação contra ataques cibernéticos e de serviço de resposta a incidentes de segurança.

A contratação pretendida está alinhada com o planejamento estratégico do CRCMG, uma vez que contribuirá para o alcance do objetivo da qualidade de "assegurar meios e recursos que possibilitem o cumprimento das políticas e diretrizes da gestão", bem como dos objetivos estratégicos de "garantir qualidade e confiabilidade nos processos e nos procedimentos".

Quantidade de serviço ou material

Grupo	Item	Descrição
1	1	Serviços de monitoramento de ataques cibernéticos
	2	Serviços de resposta a incidentes de segurança

Previsão de data em que deve ser iniciada a prestação dos serviços ou entregue o material

60 (sessenta) dias corridos após a contratação.

Indicar funcionário para compor a equipe de planejamento da contratação

Cláudio Márcio Araújo da Silva
Indicar o fiscal técnico do contrato
Cláudio Márcio Araújo da Silva
Indicar o fiscal substituto
Henry Caetano Ávila de Andrade

Validação do responsável pelo setor requisitante:

Assinado digitalmente por:
 CLAUDIO MARCIO ARAUJO DA SILVA
 CPF: 691.116.426-53
 Certificado emitido por AC SOLUTI Multipla
 Data: 17/01/2023 13:43:05 -03:00



De acordo. Encaminhe-se à Gerência Administrativa e Financeira (GEADF) para prosseguimento:

Assinado digitalmente por:
 MARIO ROGERIO MAROTTA
 CPF: 269.729.056-72
 Certificado emitido por AC SAFEWEB RFB v5
 Data: 17/01/2023 13:20:37 -03:00





MANIFESTO DE ASSINATURAS



Código de validação: DLT7A-FY6T2-FCVEA-S7XQH

Esse documento foi assinado pelos seguintes signatários nas datas indicadas (Fuso horário de Brasília):

- ✓ MARIO ROGERIO MAROTTA (CPF 269.729.056-72) em 17/01/2023 13:20 - Assinado com certificado digital ICP-Brasil
- ✓ CLAUDIO MARCIO ARAUJO DA SILVA (CPF 691.116.426-53) em 17/01/2023 13:43 - Assinado com certificado digital ICP-Brasil

Para verificar as assinaturas, acesse o link direto de validação deste documento:

<https://assinador.crcmg.org.br/validate/HLT7A-FY6T2-FCVEA-S7XQH>

Ou acesse a consulta de documentos assinados disponível no link abaixo e informe o código de validação:

<https://assinador.crcmg.org.br/validate>

ESTUDOS TÉCNICOS PRELIMINARES

Setor Requisitante	Gerência de Tecnologia da Informação
Responsável Pela Demanda	Cláudio Márcio Araújo da Silva
Equipe de Planejamento	Cláudio Márcio Araújo da Silva Henry Caetano Ávila de Andrade Izaías Angelo Gomes

1. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

Disponer de estrutura de monitoramento preventivo e contínuo de segurança da informação contra ataques cibernéticos e serviço de resposta a incidentes de segurança.

2. JUSTIFICATIVA DA NECESSIDADE DA CONTRATAÇÃO

Considerando que nos últimos anos temos visto diversas instituições públicas e privadas sofrendo constantes ataques cibernéticos, e tendo em vista a implantação da LGPD no CRCMG, que exige a adoção de medidas de segurança mais eficazes, torna-se indispensável a aplicação de boas práticas de segurança da informação no ambiente tecnológico do CRCMG, a fim de torná-lo mais seguro e menos suscetível a esses ataques.

Diante do crescimento exponencial de ameaças e ataques contra empresas privadas e órgãos públicos, no Brasil e no mundo, investimentos contínuos em segurança da informação são fundamentais para a mitigação de riscos de segurança associados ao negócio de maneira a resguardar a confidencialidade, a disponibilidade e a integridade das informações.

O cenário de ameaças à segurança da informação não se resume somente em ataques aos serviços de TI pela Internet. Tentativas de acesso não autorizado, infecção por arquivos maliciosos (vírus), e-mails indesejados (SPAMs), engenharia social, entre outros, são exemplos de eventos que podem apresentar riscos à segurança de TI. Até mesmo colaboradores não conscientes ou mal-intencionados representam risco potencial à segurança da informação.

Na busca de aperfeiçoamento da sua missão institucional e gestão pública, o Conselho Regional de Contabilidade de Minas Gerais vem utilizando cada vez mais soluções de TI, disponibilizando aos seus colaboradores, profissionais contábeis e à sociedade diversos serviços relacionados à Tecnologia da Informação. Nesse cenário, diversas foram as mudanças: tanto em termos de quantidade de serviços oferecidos quanto em diversidade de soluções, o que contribui para o aumento dos riscos e da necessidade de monitoramento, à medida que cresce a oferta de serviços pela Internet.

Nesse sentido, incidentes de segurança da informação, como nas hipóteses de violação, roubo ou perda de informações custodiadas pelo CRCMG, podem constituir possíveis situações capazes de inviabilizar, senão a totalidade, parte das atividades desta Entidade. Assim, a ocorrência de eventuais sinistros poderia provocar o vazamento de informações e prejuízo à sua imagem, podendo ainda o Conselho ter que responder por possíveis danos que venham a ser causados.

Por esses motivos, tendo em vista que o Conselho não dispõe de infraestrutura física e pessoal para o monitoramento e gerenciamento de dispositivos de segurança com diversos fornecedores (firewall, sistema de prevenção de intrusões de rede, gerenciamento unificado de ameaças), capazes de realizar ações contra incidentes de segurança de forma tempestiva e procedimental, torna-se necessária realizar a contratação de uma solução que forneça uma estrutura em segurança da informação adequada, de forma a propiciar a integridade, confidencialidade, autenticidade e a disponibilidade dos dados, através de um monitoramento preventivo e contínuo de segurança da informação contra ataques cibernéticos e de serviço de resposta a incidentes de segurança.

3. DEMONSTRAÇÃO DA PREVISÃO DA CONTRATAÇÃO NO PAC E REFERÊNCIA AOS DEMAIS INSTRUMENTOS DE PLANEJAMENTO DO CRCMG

A contratação pretendida está alinhada com o planejamento estratégico do CRCMG, uma vez que contribuirá para o alcance do objetivo da qualidade de “assegurar meios e recursos que possibilitem o cumprimento das políticas e diretrizes da gestão”, bem como dos objetivos estratégicos de “garantir qualidade e confiabilidade nos processos e nos procedimentos”.

Além disso, essa contratação está prevista no Plano Anual de Contratações e os recursos orçamentários necessários para suportar as despesas foram previstos no Plano de Trabalho do CRCMG, além de estar vinculada ao Plano Diretor de Tecnologia da Informação - PDTI.

Os recursos para custeio das despesas correrão sob a rubrica:

Conta contábil 6.3.1.3.02.01.005: Serviços de Tecnologia da Informação

Projeto 5002: Tecnologia da Informação

Justificativa: a tecnologia da informação é um instrumento primordial no gerenciamento de dados e produção de informações precisas, que possibilitem otimizar os recursos e assegurar qualidade às atividades e ao processo de tomada de decisão.

Objetivos: contratação de empresas terceirizadas de informática para o fornecimento de serviços especializados, bem como para atuar na segurança da informação.

4. REQUISITOS DA CONTRATAÇÃO

A solução de monitoramento preventivo e contínuo de segurança da informação contra ataques cibernéticos e serviço de resposta a incidentes de segurança, deverá contemplar os seguintes serviços:

- Monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados ao CONTRATANTE;
- Serviços de resposta a incidentes de segurança, para analisar, remediar, conter e documentar os eventos de segurança da informação;

- É de responsabilidade da CONTRATADA o fornecimento e instalação de todos os recursos necessários para a execução total do serviço contratado, incluindo licenças, hardwares, hospedagens, gerenciamento e suporte técnico;
- A solução ofertada deverá ter compatibilidade com todo o ambiente computacional do CRCMG.

Outros requisitos:

- A empresa contratada deve ser especializada no fornecimento do serviço requerido e nas ferramentas fornecidas para o provimento dos serviços. Todas as características e requisitos exigidos poderão ser confirmados em diligência presencial;
- A solução deve prover meios de garantir o sigilo no tráfego e no armazenamento das informações;
- A solução deve possuir mecanismos que garantam conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018);
- A empresa contratada deve comprovar qualificação técnica, por meio de atestado de capacidade técnica;
- O serviço será enquadrado como de natureza continuada considerando sua notória essencialidade para o desempenho da missão institucional do CRCMG, uma vez que irá proporcionar o monitoramento e gerenciamento de dispositivos de segurança e de provedores de detecção e resposta gerenciados, bem como reduzir os riscos de modificações acidentais ou deliberadas, acessos sem autorização ou ataques maliciosos que impactem na segurança de ativos críticos, possibilitando a segurança da informação contra ataques cibernéticos e serviço de resposta a incidentes de segurança da Entidade;
- Quanto ao prazo de vigência do contrato, com fundamento no inciso II do artigo 57 da Lei nº 8.666/1993, o qual estabelece que a prestação de serviços executados de forma contínua poderá ser prorrogada por iguais e sucessivos períodos, até o limite de 60 (sessenta) meses, sugere-se que seja fixado prazo de vigência de 60 meses contados da data de assinatura do contrato;
- A adoção do prazo de 60 meses visa proporcionar economia e eficiência para a contratação, tendo em vista que a solução a ser contratada demandará de um elevado custo de implantação, bem como tempo e esforço dos colaboradores engajados no projeto. Dessa forma, ao se estender a vigência do contrato para o período de 60 meses, será possível diluir os custos empreendidos por um período maior e reduzir os riscos de descontinuidade precoce da solução, o que demandaria novo desgaste de

tempo e recursos em uma nova implantação da solução, num pequeno período de tempo. Além disso, o período de vigência contratual mais ampliado contribui para que a contratação em tela possa ser considerada mais atrativa pelo mercado, tendo em vista que os fornecedores também poderiam diluir seus elevados custos iniciais por um período de tempo maior, estando de acordo, portanto, com os princípios da economicidade, razoabilidade, competitividade e interesse público;

- Havendo interrupção do contrato, por quaisquer motivos, deverá ser garantida a continuidade do fornecimento da solução por ocasião da transição contratual.

5. NORMATIVOS ESPECÍFICOS QUE DISCIPLINAM OS SERVIÇOS A SEREM CONTRATADOS

As condições deste estudo foram elaboradas visando atender ainda aos seguintes regramentos:

- Instrução Normativa nº 1, da Secretaria de Governo Digital/Secretaria Especial de Desburocratização, Gestão e Governo Digital/Ministério da Economia, de 4 de abril de 2019.
- Instrução Normativa nº 31, da Secretaria de Governo Digital/Secretaria Especial de Desburocratização, Gestão e Governo Digital/Ministério da Economia, de 23 de março de 2021.
- Instrução Normativa SG nº 05, de 26 de maio de 2017, que dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional.
- Lei n.º 8.666/1993, que regulamenta o Art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências.
- Lei n.º 10.520/2002, que institui, nos termos do Art. 37, inciso XXI, da Constituição Federal, a modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns.
- Decreto n.º 10.024/2019 que regulamenta a licitação, na modalidade pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns, incluídos os serviços comuns de engenharia, e dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal.
- Decreto n.º 9.507/2018, que dispõe sobre a execução indireta, mediante contratação, de serviços da administração pública federal direta, autárquica e fundacional e das empresas públicas e das sociedades de economia mista controladas pela União.

- Lei nº 14.128/2021, que dispõe sobre os princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública e altera a Lei nº 12.527/2011, a Lei nº 12.682/2012 e a Lei nº 13.460/2017.
- Portaria n.º 443/2018, que estabelece os serviços que serão preferencialmente objeto de execução indireta, em atendimento ao disposto no Art.2º do Decreto n.º 9.507, de 21 de setembro de 2018.
- Instrução Normativa nº 73, de 5 de agosto de 2020, que dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para a aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.
- Resolução CFC n.º 1.543, de 18 de outubro de 2018 - Aprova o Planejamento Estratégico do Sistema CFC/CRCs.
- Deliberação VICOI/CFC n.º 136/2022, que aprovou a proposta orçamentária do CRCMG para o exercício de 2022.
- Resolução CRCMG n.º 432/2021, aprovou o Processo Interno (PI) CRCMG n.º 17/2021, referente à Proposta Orçamentária e ao Plano de Trabalho para o exercício financeiro de 2022 do CRCMG.
- Portaria CRCMG Nº 166/2021, que aprovou o Plano Anual de Contratações de bens, serviços, obras e soluções de tecnologia da informação e comunicações do CRCMG, referente ao exercício de 2022.
- Deliberação CRCMG N.º 1.259, de 15 de dezembro de 2021, que aprovou o Plano Diretor de Tecnologia (PDTI) do CRCMG, biênio 2022/2023.
- Resolução CRCMG N.º 441, de 17 de dezembro de 2021, que aprova a Política de Segurança da Informação (PSI) do CRCMG e dá outras providências.

6. ESTIMATIVA DAS QUANTIDADES, ACOMPANHADAS DAS MEMÓRIAS DE CÁLCULO E DOS DOCUMENTOS QUE LHE DÃO SUPORTE, QUE CONSIDEREM INTERDEPENDÊNCIAS COM OUTRAS CONTRATAÇÕES, DE MODO A POSSIBILITAR ECONOMIA DE ESCALA

Grupo	Item	Descrição	Quantidade	Unidade
1	1	Serviços de monitoramento de ataques cibernéticos	60	meses
	2	Serviços de resposta a incidentes de segurança	60	meses

Todos os itens acima pertencem a um único objeto e bloco de contratação, compreendendo o fornecimento de SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO (MSS – Managed Security Services), sendo expressamente vedada a subcontratação total ou parcial do objeto.

Para efeitos de estimativa de volume, os fornecedores deverão considerar os seguintes números baseados no ambiente tecnológico do CRCMG, sendo no total 134 ativos:

1. Colaboradores: 86

2. Estações de trabalho:

- i. Desktop: 96
- ii. Notebook: 30

3. Servidores Linux: 4, sendo:

- i. Servidor MySQL e Nginx

4. Servidores Windows: 4, sendo:

- i. Servidor SQL Server: 1
- ii. Servidor IIS: 1
- iii. Servidor AD: 1
- iv. File Server: 1

5. Links de comunicação:

- i. Links de internet: 2 (dois), com 50 Mbps cada;
- ii. Links de dados entre Datacenter e CRCMG: 2 (dois), 40 Mbps cada.

6. Antivírus: Cylance

7. Firewall: Fortnet – Gerenciamento prestado por empresa terceirizada

7. ANÁLISE DA CONTRATAÇÃO ANTERIOR

Não se aplica.

8. LEVANTAMENTO DE MERCADO, QUE CONSISTE NA ANÁLISE DAS ALTERNATIVAS POSSÍVEIS, E JUSTIFICATIVA TÉCNICA E ECONÔMICA DA ESCOLHA DO TIPO DE SOLUÇÃO A CONTRATAR

Para este levantamento foram analisadas contratações similares feitas por outros órgãos integrantes do sistema CFC/CRCs, por meio de pesquisa dos contratos em seus respectivos portais da transparência, além de busca por empresa especializada em monitoramento de segurança da informação, com objetivo de identificar a existência de novas metodologias, tecnologias ou inovações que melhor atendam às necessidades da Administração, tendo sido levantadas as seguintes soluções:

Aquisição ou subscrição de ferramentas de segurança:

Essa solução consiste na aquisição ou subscrição de ferramentas para atender aos requisitos técnicos definidos na especificação. Para isso, adicionalmente, será necessário realizar o treinamento, implantação, administração e uso coordenado de todas essas ferramentas especializadas adquiridas.

Contratação de empresa de prestação de serviços terceirizados com alocação de mão de obra:

Essa solução consiste na contratação de empresa de prestação de serviços terceirizados de mão de obra, para fornecer ao CRCMG 1 analista de segurança com a experiência e qualificações necessárias para realizar os serviços. Para isso, seria necessário realizar um processo licitatório para a contratação dessa empresa e, adicionalmente, seria necessário a aquisição ou subscrição de ferramentas para atender aos requisitos técnicos definidos nas especificações do objeto deste processo, além de treinamento, implantação, administração e uso coordenado de todas essas ferramentas especializadas.

Contratação de empresa especializada para realizar a prestação dos serviços:

Essa solução consiste na contratação de empresa especializada, contemplando serviços gerenciados de segurança da informação, incluindo softwares e suas licenças, gerenciamento centralizado, serviços de implantação, garantia de atualização contínua e suporte técnico. Este modelo é viável, sob o ponto de vista técnico, além de ser prática amplamente adotada no mercado. Integrada por coletânea de serviços voltados a reduzir riscos e a diminuir a lacuna de habilidades de segurança da entidade. Os serviços proporcionam o monitoramento de segurança e gerenciamento de dispositivos de segurança com diversos fornecedores (firewall, sistema de prevenção de intrusões de rede, gerenciamento unificado de ameaças e etc.) como também, provedores de detecção e resposta gerenciados. A solução tem como proposta reduzir os riscos de modificações acidentais ou deliberadas, acessos sem autorização ou ataques maliciosos que impactem na segurança de ativos críticos. O monitoramento é fornecido por meio de SOCs ("Security Operations Center", Centro de Operações de Segurança), que reúne infraestrutura física e pessoal responsável por administrar e monitorar sistemas de segurança de TI, de maneira remota, em regime de operação 24x7 (24 horas por dia, 7 dias por semana), capazes de realizar ações contra incidentes de segurança de forma tempestiva e procedimental.

Dessa forma, considerando todas as alternativas levantadas, entendemos que a solução mais adequada para o atendimento dos requisitos do objeto deste estudo é a **contratação de empresa especializada para realizar a prestação dos serviços**, uma vez que as outras alternativas levantadas são inviáveis para o Conselho, tendo em vista os motivos citados abaixo:

Em virtude do cenário atual da equipe de TI do CRCMG, relativo ao quantitativo de pessoal e à jornada de trabalho (dentro do horário de expediente), a **aquisição ou subscrição de ferramentas** para atender aos requisitos técnicos definidos não resolveria o problema, uma vez que o monitoramento e gerenciamento de dispositivos de segurança necessita de uma infraestrutura física para administrar e monitorar os sistemas de segurança de maneira remota, em regime de operação 24x7 (24 horas por dia, 7 dias por semana), tornando impossível o atendimento à demanda por meio dessa alternativa.

Com relação à **contratação de empresa de prestação de serviços terceirizados com alocação de mão de obra**, levando em conta o aspecto técnico e de gestão do serviço, julgamos inviável devido aos riscos envolvidos neste tipo de contratação, uma vez que impossibilitaria a atribuição objetiva de responsabilidades da contratada, inviabilizando o atingimento da finalidade da contratação, que é a adequada coordenação de ações para a proteção do ambiente, a prevenção de ataques de segurança da informação e a rápida resposta para eventuais comprometimentos.

Outro aspecto avaliado, agora sob o ponto de vista de custo mensal do serviço, será a vigência do contrato, tendo em vista que a contratada será responsável pelo investimento na aquisição de equipamentos, produtos e licenças necessárias na prestação do serviço, e dessa forma é de se esperar que o custo mensal para um serviço de 60 meses seja menor do que o custo mensal de um serviço de 12 meses, devido à diluição dos custos do investimento inicial, o que será ou não validado nas pesquisas de mercado.

Vale ressaltar também que não serão necessárias adequações prévias do ambiente do CRCMG para a execução do serviço, seja sob o aspecto físico, uma vez que os serviços serão prestados remotamente, seja sob o aspecto de software e hardware, que utilizarão os recursos atualmente existentes no ambiente local.

Portanto, considerando o exposto, foi possível constatar que a **contratação de empresa especializada para realizar a prestação dos serviços** é o tipo de solução mais adequado e praticado por entidades da Administração Pública, no qual o fornecedor se responsabiliza por toda a estrutura necessária à disponibilização do serviço e o cliente paga um valor mensal ou anual pelos serviços.

Algumas vantagens desse modelo de contratação são:

- ✓ Serviços dessa natureza são, usualmente, prestados por empresas especializadas em segurança da informação atuantes no mercado de MSSP (Managed Security Services Provider), as quais oferecem serviços de monitoração contínua de segurança da informação por meio de SOCs (Security Operation Centers).
- ✓ Tais empresas possuem infraestruturas físicas e softwares adequados e equipe especializada e certificada que monitora o ambiente de TI, de maneira remota, em regime de operação 24x7 (24 horas por dia, 7 dias por semana), aplicando as ações necessárias contra os incidentes de segurança identificados.
- ✓ O serviço especializado de segurança da informação trabalha em horário integral, durante todos os dias do ano, tornando-o, dessa forma, mais efetivo se comparado ao profissional exercendo a atividade de segurança da informação apenas em horário comercial no CRCMG.
- ✓ As empresas prestadoras de serviço de segurança comercializam serviços segundo as necessidades particulares de cada cliente e oferecem no mercado pacotes de serviços diferenciados, de acordo com o dimensionamento, risco, abrangência e valor do investimento.

Por fim, ao pesquisar contratações de outros órgãos e entidades da administração pública com estrutura similar à do CRCMG, foi possível constatar que o modelo vem sendo implementado sistematicamente pelas organizações públicas, o que pode ser exemplificado por meio dos processos abaixo listados:

- Edital Pregão Eletrônico N.º 011/2021 - Conselho Regional de Contabilidade de São Paulo;

- Edital Pregão Eletrônico N.º 06/2022 - Conselho Federal de Contabilidade;
- Edital Pregão Eletrônico N.º 20/2021 - Conselho Nacional do Ministério Público;
- Edital Pregão Eletrônico N.º 11/2021 - Comissão de Valores Mobiliários;
- Edital Pregão Eletrônico N.º 043/2021 - Superior Tribunal de Justiça;
- Edital Pregão Eletrônico N.º 03/2021 - Conselho Nacional de Justiça;

9. ESTIMATIVA DO VALOR DA CONTRATAÇÃO, ACOMPANHADAS DAS MEMÓRIAS DE CÁLCULO E DOS DOCUMENTOS QUE LHESS DÃO SUPORTE, QUE CONSIDEREM INTERDEPENDÊNCIAS COM OUTRAS CONTRATAÇÕES, DE MODO A POSSIBILITAR ECONOMIA DE ESCALA

9.1. Foram realizadas pesquisas preços nos termos da Instrução Normativa Seges nº 73, de 5 de agosto de 2020, adotando-se como parâmetro pesquisas sobre contratações similares de outros entes públicos, conforme quadro demonstrativo abaixo:

CONTRATAÇÕES DA ADMINISTRAÇÃO PÚBLICA			
ORGÃOS/ENTIDADES DA ADMINISTRAÇÃO PÚBLICA			
CONSELHO FEDERAL DE CONTABILIDADE	CONSELHO REGIONAL DE CONTABILIDADE DO ESTADO DE SÃO PAULO	TRIBUNAL REGIONAL DO TRABALHO DA 17.ª REGIÃO	TRIBUNAL REGIONAL FEDERAL DA 3ª REGIÃO
EMPRESAS CONTRATADAS			
ISH TECNOLOGIA S/A.	ISH TECNOLOGIA S/A.	Intelliway Tecnologia LTDA	S3CURITY TECNOLOGIA SERVIÇOS DE INFORMÁTICA LTDA
Mensal	Mensal	Mensal	Mensal
R\$ 14.537,50	R\$ 35.500,00	R\$ 101.825,00	R\$ 78.000,00

9.2. Diante das pesquisas obtidas, será utilizada como metodologia para obtenção do preço estimado o menor valor apurado entre as contratações da Administração Pública, que corresponde ao contrato firmado entre o Conselho Federal de Contabilidade e a empresa ISH Tecnologia S/A.

9.3. Assim, considerando que a contratação se estenderá pelo período de 60 (sessenta) meses, o valor global estimado será de R\$ 872.250,00 (oitocentos e setenta e dois mil duzentos e cinquenta reais).

VALOR DE REFERÊNCIA	
Estimativa Mensal	Estimativa Global 60 meses
R\$ 14.537,50	R\$ 872.250,00

10. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO, INCLUSIVE DAS EXIGÊNCIAS RELACIONADAS À MANUTENÇÃO E À ASSISTÊNCIA TÉCNICA, QUANDO FOR O CASO

A solução a ser contratada deverá contemplar os seguintes serviços:

Serviços de monitoramento de ataques cibernéticos: visa o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados ao CONTRATANTE, através de correlacionamento de logs, pacotes de redes, e/ou comportamento anômalo de aplicações, serviços e infraestrutura do CONTRATANTE, que possam gerar eventos de segurança da informação, aos quais devem ser analisados, podendo estes serem transformados em um incidente de segurança da informação, obedecendo um processo cíclico e rigoroso de gestão de eventos;

Serviços de resposta a incidentes de segurança: para analisar, remediar, conter e documentar os eventos de segurança da informação, que após analisados se descobriu que de fato era um ataque iminente ao CONTRATANTE, e foram transformados em um incidente de segurança da informação. Tal serviço deverá ser executado através de um SOC ("Security Operations Center", Centro de Operações de Segurança), obedecendo os principais frameworks de resposta a incidente de segurança da informação, e boas práticas de mercado já conhecidas;

Todos os serviços descritos pertencem a um único objeto e bloco de contratação denominado **SERVIÇOS GERENCIADOS DE SEGURANÇA**. Todas as características e requisitos exigidos nesse termo de referência poderão ser confirmadas em diligência presencial;

É de responsabilidade da CONTRATADA o fornecimento e instalação de todos os recursos necessários para a execução total do serviço contratado, incluindo licenças, hardwares, hospedagens, gerenciamento e suporte técnico;

A empresa contratada deve ser especializada no fornecimento do serviço requerido e nas ferramentas fornecidas para o provimento dos serviços, devendo a solução ofertada ter compatibilidade com todo o ambiente computacional do CRCMG;

O contrato terá o prazo de vigência de 60 (sessenta) meses, contados da data de assinatura;

11. JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO, QUANDO NECESSÁRIA PARA A INDIVIDUALIZAÇÃO DO OBJETO

Por se tratar de uma solução tecnicamente indivisível, os recursos e serviços que irão compor o objeto do processo de contratação deverão ser contratados por meio de empreitada por preço global, correspondendo em sua totalidade a um único item na licitação, de forma a assegurar a total integração e assim evitar qualquer prejuízo para o conjunto da solução e dissolução de responsabilidades.

Nesse sentido, com base no levantamento efetuado no mercado, é possível afirmar que a aglutinação dos recursos pretendidos em uma única solução não prejudicará a ampla

participação de licitantes, tendo em vista que os fornecedores especializados na prestação deste serviço possuem capacidade técnica e operacional para execução da totalidade do objeto.

12. DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS EM TERMOS DE ECONOMICIDADE E DE MELHOR APROVEITAMENTO DOS RECURSOS HUMANOS, MATERIAIS OU FINANCEIROS DISPONÍVEIS

Conforme abordado anteriormente, a monitoração preventiva e contínua de segurança da informação tornou-se um elemento indispensável para a consecução da missão institucional dessa Entidade, de modo a evitar o vazamento ou perda de informações, além de demandar tempo e custo significativos de retorno às operações normais.

Nesse sentido, por meio dessa contratação pretende-se minimizar os riscos de ataques cibernéticos, profissionalizar a capacidade de resposta a incidentes de segurança em TI e atender aos requisitos de segurança da informação.

Assim, além de contribuir para a consecução dos objetivos estratégicos do Conselho fica evidenciado o interesse público, em termos de economicidade, eficácia, eficiência e de melhor aproveitamento dos recursos humanos, materiais e financeiros disponíveis, o que contribui, conseqüentemente, para a melhoria da qualidade de produtos ou serviços oferecidos à sociedade.

13. PROVIDÊNCIAS A SEREM ADOTADAS PELA ADMINISTRAÇÃO PREVIAMENTE À CELEBRAÇÃO DO CONTRATO, INCLUSIVE QUANTO À CAPACITAÇÃO DE SERVIDORES OU DE EMPREGADOS PARA FISCALIZAÇÃO E GESTÃO CONTRATUAL

Considerando que para a prestação desses serviços já existe a infraestrutura adequada no Conselho, não será necessário adotar nenhuma providência.

14. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

Não se aplica.

15. DESCRIÇÃO DE POSSÍVEIS IMPACTOS AMBIENTAIS E RESPECTIVAS MEDIDAS MITIGADORAS, INCLUÍDOS REQUISITOS DE BAIXO CONSUMO DE ENERGIA E DE OUTROS RECURSOS, BEM COMO LOGÍSTICA REVERSA PARA DESFAZIMENTO E RECICLAGEM DE BENS E REFUGOS, QUANDO APLICÁVEL

Não se aplica.

16. POSICIONAMENTO CONCLUSIVO SOBRE A ADEQUAÇÃO DA CONTRATAÇÃO PARA O ATENDIMENTO DA NECESSIDADE A QUE SE DESTINA

Diante dos elementos consignados neste estudo, foi possível constatar que o objeto da contratação em epígrafe está alinhado com o Planejamento Estratégico do CRCMG e com o interesse público, que há recursos orçamentários suficientes à cobertura das despesas correspondentes, tendo em vista a previsibilidade da contratação no Plano de Trabalho, PDTI e Plano Anual de Contratações do CRCMG, e que a solução escolhida está de acordo com a prática de mercado, havendo fornecedores qualificados para prestar os serviços na forma pretendida.

Assim, a equipe de planejamento declara que a contratação, objeto deste estudo, é viável sob os aspectos econômicos, de conveniência e oportunidade.

Assinado digitalmente por:
CLAUDIO MARCIO ARAUJO DA SILVA
CPF: 691.116.426-53
Certificado emitido por AC SOLUTI Multipla
Data: 19/01/2023 11:00:59 -03:00



Cláudio Márcio Araújo da Silva
Membro

Assinado digitalmente por:
HENRY CAETANO AVILA DE ANDRADE
CPF: 059.963.316-67
Certificado emitido por AC VALID RFB v5
Data: 19/01/2023 13:59:21 -03:00



Henry Caetano Ávila de Andrade
Membro

Assinado digitalmente por:
IZAIAS ANGELO GOMES
CPF: 046.926.156-05
Certificado emitido por AC SOLUTI Multipla v5
Data: 19/01/2023 09:48:18 -03:00



Izaías Angelo Gomes
Membro



MANIFESTO DE ASSINATURAS



Código de validação: GJM9Q-LDJLZ-CSSD7-RB5N6

Esse documento foi assinado pelos seguintes signatários nas datas indicadas (Fuso horário de Brasília):

- ✓ IZAIAS ANGELO GOMES (CPF 046.926.156-05) em 19/01/2023 09:48 -
Assinado com certificado digital ICP-Brasil
- ✓ CLAUDIO MARCIO ARAUJO DA SILVA (CPF 691.116.426-53) em 19/01/2023
11:00 - Assinado com certificado digital ICP-Brasil
- ✓ HENRY CAETANO AVILA DE ANDRADE (CPF 059.963.316-67) em 19/01/2023
13:59 - Assinado com certificado digital ICP-Brasil

Para verificar as assinaturas, acesse o link direto de validação deste documento:

<https://assinador.crcmg.org.br/validate/GJM9Q-LDJLZ-CSSD7-RB5N6>

Ou acesse a consulta de documentos assinados disponível no link abaixo e informe o código de validação:

<https://assinador.crcmg.org.br/validate>

MAPA DE RISCOS											
Objeto		Contratação de serviços de monitoramento preventivo e contínuo de segurança da informação contra ataques cibernéticos e serviço de resposta a incidentes de segurança.									
Equipe de Planejamento		Cláudio Márcio Araújo da Silva Henry Caetano Ávila de Andrade Izaías Angelo Gomes									
FASE DA ANÁLISE											
(X) Planejamento da contratação () Seleção do fornecedor () Execução do Contrato											
Nº	Risco	Consequência	Tipo	Avaliação				Estratégia para eliminar ou minimizar a ocorrência do risco		Estratégia de contingência caso o risco se concretize	
				SEVERIDADE	ABRANGÊNCIA	FREQUENCIA	CLASSE	Ação	Responsável	Ação	Responsável
1	Descrição de serviços com tecnologia defasada.	Contratação de serviços que não atendam aos critérios de segurança e modernidade, podendo resultar em ineficiência da prestação.	Interno	2	1	2	4	Análise consistente entre as opções disponíveis no mercado, observadas as necessidades da Administração.	Getin	Analisar a possibilidade de adequação dos serviços, dentro dos limites permitidos na lei.	Getin/ Presidência
2	Estabelecimento de especificações que extrapolam a real necessidade da solução e de opções disponíveis no mercado.	Impugnação ao edital. Licitação fracassada ou deserta.	Interno	2	1	1	2	Ao elaborar o termo de referência, verificar as especificações de serviços contratados por outros órgãos da Administração Pública.	Getin	Havendo impugnação que deva ser acatada, promover as alterações que forem pertinentes. Havendo licitação fracassada ou deserta,	Getin/ Presidência

Rua Cláudio Manoel, 639 - Bairro Savassi

 Esse documento foi assinado por IZAIAS ANGELO GOMES, CLAUDIO MARCIO ARAUJO DA SILVA, HENRY CAETANO AVILA DE ANDRADE e IZAIAS ANGELO GOMES. Para validar o documento e suas assinaturas acesse <https://assinador.crcmg.org.br/validate/EYQBT-H5M3S-SSDGX-GWUQH>

 crcmg@crcmg.org.br – www.crcmg.org.br

										verificar os motivos que levaram à sua ocorrência e promover os ajustes necessários.	

A identificação, análise, avaliação e tratamento dos riscos dos processos de contratação do CRCMG são realizados em consonância com o Procedimento Geral PG-007/SQ – Gestão de riscos e oportunidades, considerando que o CRCMG possui uma Política de Gestão de Riscos instituída, conforme Portaria CRCMG nº 132/2017, bem como observando os critérios estabelecidos pela Instrução Normativa SG/MPDG nº 05/2017.

Abrangência:

- 1: Local - Afeta aquele processo especificamente a que está relacionado.
- 2: Adjacente - Afeta mais de um processo.
- 3: Global - Afeta vários processos, internos e externos, impactando o Sistema de Gestão da Qualidade.

Frequência:

- 1: Rara - A ocorrência daquela falha é pequena.
- 2: Eventual - A ocorrência daquela falha é ocasional.
- 3: Frequente - A falha ocorre sempre, por diversas vezes.

Severidade:

- 1: Baixa - Levemente prejudicial. Impactos que não comprometem substancialmente o desenvolvimento do processo.
- 2: Moderada - Prejudicial. Impactos que comprometem o desenvolvimento do processo ou o atendimento aos objetivos.
- 3: Alta - Extremamente prejudicial. Impactos que comprometem substancialmente o desenvolvimento do processo, bem como o atendimento aos objetivos.

Classificação do risco

A classificação do risco consiste na multiplicação dos valores atribuídos aos fatores severidade, abrangência e frequência: $CLASSE = SEVERIDADE \times ABRANGÊNCIA \times FREQUÊNCIA$.

A pontuação mínima possível a um determinado impacto é 1 (1 x 1 x 1), indicando que o aspecto não provoca qualquer efeito adverso. A pontuação máxima possível é 27 (3 x 3 x 3), o que significa que o aspecto é extremamente prejudicial.

A classificação do impacto em ser ou não significativo obedece ao agrupamento definido abaixo:

- Resultado de 1 a 4: Risco tolerável.
 Resultado de 6 a 12: Risco moderado.
 Resultado de 18 a 27: Risco crítico.

Rua Cláudio Manoel, 639 - Bairro Savassi
 Telefone: (31) 3269-8400 – CEP: 30140-105 – Belo Horizonte/MG

crcmg@crcmg.org.br – www.crcmg.org.br

Esse documento foi assinado por IZAIAS ANGELO GOMES, CLAUDIO MARCIO ARAUJO DA SILVA e HENRY CAETANO AVILA DE ANDRADE. Para validar o documento e suas assinaturas acesse <https://assinador.crcmg.org.br/validate/EYQBT-H5M3S-SSDGX-GWUQH>

Os riscos externos e os riscos internos classificados como toleráveis não requerem uma ação específica de tratamento, devendo ser monitorados.

Cabe à Comissão de Governança, Riscos e Compliance realizar a priorização dos riscos classificados como críticos e moderados, classificando aqueles que são considerados riscos-chave e avaliando a necessidade de abertura de plano de ação, e levar à aprovação do Conselho Diretor.

Tratamento do risco:

O tratamento de riscos envolve a seleção de uma ou mais opções para modificar os riscos e a implementação dessas opções, que podem ser, entre outras:

- a) aceitar o risco;
- b) transferir ou compartilhar o risco com outra parte;
- c) evitar o risco pela decisão de descontinuar ou não iniciar a atividade;
- d) abrir plano de ação para mitigar ou reduzir o risco.

Assinado digitalmente por:
CLAUDIO MARCIO ARAUJO DA SILVA
CPF: 691.116.426-53
Certificado emitido por AC SOLUTI Multipla
Data: 19/01/2023 11:00:05 -03:00



Cláudio Márcio Araújo da Silva
Membro

Assinado digitalmente por:
HENRY CAETANO ÁVILA DE ANDRADE
CPF: 059.963.316-67
Certificado emitido por AC VALID RFB v5
Data: 19/01/2023 14:00:05 -03:00



Henry Caetano Ávila de Andrade
Membro

Assinado digitalmente por:
IZAIAS ANGELO GOMES
CPF: 046.926.156-05
Certificado emitido por AC SOLUTI Multipla v5
Data: 19/01/2023 09:32:16 -03:00



Izaías Angelo Gomes
Membro

Rua Cláudio Manoel, 639 - Bairro Savassi
Telefone: (31) 3269-8400 – CEP: 30140-105 – Belo Horizonte/MG

crmg@crmg.org.br – www.crcmg.org.br

Esse documento foi assinado por IZAIAS ANGELO GOMES, CLAUDIO MARCIO ARAUJO DA SILVA e HENRY CAETANO AVILA DE ANDRADE. Para validar o documento e suas assinaturas acesse <https://assinador.crcmg.org.br/validate/EYQBT-H5M3S-SSDGX-GWUQH>



MANIFESTO DE ASSINATURAS



Código de validação: EYQBT-H5M3S-SSDGX-GWUQH

Esse documento foi assinado pelos seguintes signatários nas datas indicadas (Fuso horário de Brasília):

- ✓ IZAIAS ANGELO GOMES (CPF 046.926.156-05) em 19/01/2023 09:32 -
Assinado com certificado digital ICP-Brasil
- ✓ CLAUDIO MARCIO ARAUJO DA SILVA (CPF 691.116.426-53) em 19/01/2023
11:00 - Assinado com certificado digital ICP-Brasil
- ✓ HENRY CAETANO AVILA DE ANDRADE (CPF 059.963.316-67) em 19/01/2023
14:00 - Assinado com certificado digital ICP-Brasil

Para verificar as assinaturas, acesse o link direto de validação deste documento:

<https://assinador.crcmg.org.br/validate/EYQBT-H5M3S-SSDGX-GWUQH>

Ou acesse a consulta de documentos assinados disponível no link abaixo e informe o código de validação:

<https://assinador.crcmg.org.br/validate>

TERMO DE REFERÊNCIA

1. DO OBJETO

Contratação de empresa especializada em SERVIÇOS GERENCIADOS DE SEGURANÇA.

2. INDICAÇÃO DE RECURSOS ORÇAMENTÁRIOS

Centro de Custo: 327

Projeto: 5002

Conta contábil: 6.3.1.3.02.01.005

3. JUSTIFICATIVA DO INTERESSE PÚBLICO EVIDENCIADO

Considerando que nos últimos anos temos visto diversas instituições públicas e privadas sofrendo constantes ataques cibernéticos, e tendo em vista a implantação da LGPD no CRCMG, que exige a adoção de medidas de segurança mais eficazes, torna-se indispensável a aplicação de boas práticas de segurança da informação no ambiente tecnológico do CRCMG, a fim de torna-lo mais seguro e menos suscetível a esses ataques.

Diante do crescimento exponencial de ameaças e ataques contra empresas privadas e órgãos públicos, no Brasil e no mundo, investimentos contínuos em segurança da informação são fundamentais para a mitigação de riscos de segurança associados ao negócio de maneira a resguardar a confidencialidade, a disponibilidade e a integridade das informações.

O cenário de ameaças à segurança da informação não se resume somente em ataques aos serviços de TI pela Internet. Tentativas de acesso não autorizado, infecção por arquivos maliciosos (vírus), e-mails indesejados (SPAMs), engenharia social, entre outros, são exemplos de eventos que podem apresentar riscos à segurança de TI. Até mesmo colaboradores não conscientes ou mal-intencionados representam risco potencial à segurança da informação.

Na busca de aperfeiçoamento da sua missão institucional e gestão pública, o Conselho Regional de Contabilidade de Minas Gerais vem utilizando cada vez mais soluções de TI, disponibilizando aos seus colaboradores, profissionais contábeis e à sociedade diversos serviços relacionados à Tecnologia da Informação. Nesse cenário, diversas foram as mudanças: tanto em termos de quantidade de serviços oferecidos quanto em diversidade de soluções, o que contribui para o aumento dos riscos e da necessidade de monitoramento, à medida que cresce a oferta de serviços pela Internet.

Nesse sentido, incidentes de segurança da informação, como nas hipóteses de violação, roubo ou perda de informações custodiadas pelo CRCMG, podem constituir possíveis situações capazes de inviabilizar, senão a totalidade, parte das atividades desta Entidade. Assim, a ocorrência de eventuais sinistros poderia provocar o vazamento de informações e prejuízo à sua imagem, podendo ainda o Conselho ter que responder por possíveis danos que venham a ser causados.

Por esses motivos, tendo em vista que o Conselho não dispõe de infraestrutura física e pessoal para o monitoramento e gerenciamento de dispositivos de segurança com diversos fornecedores (firewall, sistema de prevenção de intrusões de rede, gerenciamento unificado de ameaças), capazes de realizar ações contra incidentes de segurança de forma tempestiva e procedimental, torna-se necessária realizar a contratação de uma solução que forneça uma estrutura em segurança da informação adequada, de forma a propiciar a integridade, confidencialidade, autenticidade e a disponibilidade dos dados, através de um monitoramento

preventivo e contínuo de segurança da informação contra ataques cibernéticos e de serviço de resposta a incidentes de segurança.

4. AMBIENTE TECNOLÓGICO DA CONTRATANTE (HARDWARE E SOFTWARE)

Infraestrutura tecnológica:

- 1 Firewall + 1 centralizador de logs, registros e relatórios como serviço;
- 129 estações de trabalho;
- 7 servidores virtuais Windows;
- 4 servidores virtuais Linux
- 90 usuários de rede;
- 125 caixas de e-mail na GSuite;

5. ESCOPO DOS SERVIÇOS

5.1. Serviços de monitoramento de ataques cibernéticos e resposta a incidentes:

- 5.1.1. Visa o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados à CONTRATANTE, através de fornecimento de solução de correlacionamento de logs de aplicações, serviços e infraestrutura do CONTRATANTE, que possam gerar eventos de segurança da informação, aos quais devem ser analisados, remediados, contidos e documentados, podendo estes serem transformados em um incidente de segurança da informação, obedecendo um processo cíclico e rigoroso de gestão de eventos.

5.2. Serviços de Gestão de Vulnerabilidades:

- 5.2.1. Tem por objetivo, de forma proativa e recorrente, identificar possíveis vulnerabilidades de segurança da informação na infraestrutura, nas aplicações e nas contas de usuários do CONTRATANTE, a fim de evitar que ataques cibernéticos direcionados à CONTRATANTE obtenha sucesso, explorando tais vulnerabilidades já conhecidas.

5.3. Serviço de monitoramento, detecção e resposta a incidentes para Endpoints.

- 5.3.1. Visa a proteção, monitoramento contínuo e operação de solução dedicada a proteção de estações e servidores do CONTRATANTE, realizando de forma proativa o bloqueio de códigos maliciosos tipo vírus, Malware - blindando os ativos protegidos também contra Ransomware, oferecendo possibilidade de realização de "Rollback" de arquivos alvos de códigos maliciosos, oferecendo ainda suporte à investigação de ataques através da trilha de registros de eventos forense.

6. REQUISITOS GERAIS DOS SERVIÇOS

- 6.1. Os requisitos gerais dos serviços definem os requisitos obrigatórios para todos os serviços que compõem o objeto SERVIÇOS GERENCIADOS DE SEGURANÇA.

- 6.1.1. A CONTRATADA deverá cumprir com os prazos de detalhamento e as informações com a periodicidade referenciada neste documento, segmentados pelas modalidades de prestação

de serviço.

6.1.2. Todos os entregáveis mensais referenciados neste documento, a partir do terceiro mês de contrato, deverão ser exibidos comparando com os dois meses anteriores para comparação gráfica de evolução e desempenho.

6.2. São apresentadas, a seguir, as especificações técnicas mínimas dos serviços a serem ofertados referentes ao objeto. Os termos “possui”, “permite”, “suporta” e “é” implicam no fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo “ou” implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo “e” implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções.

6.3. A CONTRATADA deverá possuir ao menos 01 (um) Centro de operação de segurança, atendendo, no mínimo, as seguintes características:

6.4. CANAIS DE COMUNICAÇÃO

6.4.1. Para abertura de solicitações, a CONTRATADA deverá disponibilizar 03 (três) tipos de canais de comunicação, a saber:

Grupo de Tecnologia	Classificação
Linha telefônica	Tipo 1
E-mail com domínio registrado e de propriedade da CONTRATADA.	Tipo 2
Sistema de ITSM do inglês <i>Information Technology Service Management</i> (Gerenciamento de Serviços de TI).	Tipo 3

Tabela 1- Tipos de canais de comunicação

6.4.2. Independente do canal de comunicação utilizado pela CONTRATANTE, as solicitações devem ser convergidas, atualizadas, resolvidas e concentradas em um único sistema de ITSM (Gerenciamento de Serviços de TI). Ou seja, imaginando que a CONTRATANTE realize a abertura de uma nova solicitação de serviço via linha telefônica, no segundo que segue a sua solicitação, a mesma deve constar no sistema de ITSM, assim também deve se proceder com a utilização do canal de comunicação do tipo 2: via e-mail.

6.4.3. Sobre o canal de comunicação do tipo 1: via linha telefonia tais ligações obrigatoriamente devem ser atendidas e/ou recepcionadas por uma interface humana, não sendo permitida a utilização de URA (Unidade de Resposta Audível), e/ou qualquer uso de atendimento eletrônico.

6.4.4. Para um eventual cenário de crise, ou seja, onde o negócio fim da CONTRATANTE estiver sendo fortemente afetado por um problema envolvendo a segurança da informação, a CONTRATADA deverá disponibilizar uma sala de videoconferência virtual de sua propriedade, onde a qualquer tempo poderá ser utilizada para reuniões emergenciais para tratamento de crises.

- 6.4.5. Tal sala deve estar disponível via internet e seu acesso deve obrigatoriamente ser criptografado, utilizando protocolo SSL do inglês Secure Socket Layer, com certificado digital emitido em nome da CONTRATADA. A CONTRATADA também deve garantir que os canais de comunicação utilizados pela sala de videoconferência utilizem protocolos para criptografia dos dados trafegados.
- 6.4.6. A sala virtual ainda deve ter capacidade para minimamente 10 (dez) pessoas da CONTRATANTE simultaneamente, e a fim de evitar eventuais perdas de tempo em momento de crise, a sala deve estar acessível a qualquer tempo, não sendo criada apenas no momento da crise.

6.5. HORÁRIO DE ATENDIMENTO

- 6.5.1. Os SERVIÇOS GERENCIADOS DE SEGURANÇA devem obrigatoriamente ser executados, ofertados e estar acessíveis à CONTRATANTE em regime de 24 (vinte quatro) horas por dia, 07 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, durante todo o período de vigência do contrato.
- 6.5.2. Todo o atendimento deve ser iniciado por profissionais da contratada que estejam em horário de trabalho no momento do atendimento. Não é permitido o uso de funcionários no chamado "Regime de Plantão", "Sobreaviso" e/ou sistemas similares onde o funcionário apenas passa a trabalhar no momento do incidente.
- 6.5.3. GESTÃO DE CATÁLOGO DE SERVIÇO DO AMBIENTE DE SEGURANÇA DA INFORMAÇÃO**
- 6.5.3.1. A fim de fornecer uma única fonte de informação sobre os SERVIÇOS GERENCIADOS DE SEGURANÇA, disponíveis para cada grupo de tecnologia dos itens de configuração do parque de segurança da informação da CONTRATANTE, será definido em conjunto com a CONTRATADA uma lista de serviços que a CONTRATADA deverá ser capaz de entregar. Tal definição deverá ser aceita por ambas as partes e ficar disponível para consulta.
- 6.5.3.2. É de responsabilidade da CONTRATADA manter, atualizar e revisar os serviços disponíveis para cada grupo de serviço. As responsabilidades da CONTRATANTE estão relacionadas a aprovação de um novo serviço, ou a aposentadoria de um ou mais serviços existentes.
- 6.5.3.3. O catálogo de serviço deverá ser mantido e administrado através do sistema de ITSM de responsabilidade da CONTRATADA, estando este disponível de forma online para a CONTRATANTE, onde essa poderá consultar, a qualquer tempo, os serviços disponíveis.
- 6.5.3.4. Apesar de já existir uma definição prévia de parte dos serviços a serem entregues pela CONTRATADA, incluídas no presente termo de referência (**Anexo VII - CATÁLOGO DE SERVIÇO**), a CONTRATANTE, a qualquer tempo, poderá solicitar a inclusão de novos serviços, ou a retirada de um serviço, em comum acordo com a CONTRATADA.
- 6.5.3.5. Também se espera que tais revisões de continuidade de um serviço no catálogo de serviços seja sugerido por parte da CONTRATADA durante a execução do contrato. Todavia, não é

de responsabilidade da CONTRATADA a retirada ou inclusão de um serviço, cabendo apenas à CONTRATANTE tal ação.

6.5.4. MODALIDADE DE ATENDIMENTO

- 6.5.4.1. A modalidade preferencial de atendimento será a do tipo remota, devendo ser realizada nas dependências da CONTRATADA caso necessário, obedecendo, obrigatoriamente, os critérios estabelecidos para sua execução, conforme previstos neste Termo de Referência.
- 6.5.4.2. Os atendimentos referentes ao objeto contratado, denominado SERVIÇOS GERENCIADOS DE SEGURANÇA, são ilimitados durante o período de vigência do contrato, ou seja, não existe limite para quantidade de horas, e/ou quantidade de atendimentos realizados, limitando-se apenas ao escopo.

6.5.5. ACESSIBILIDADE E CONFIDENCIALIDADE

- 6.5.5.1. Para garantir a qualidade e disponibilidade dos serviços remotos, entre a CONTRATANTE e o Centro de Operações de Segurança da CONTRATADA, deverá haver dois tipos de conexões digitais, a fim de garantir a redundância e disponibilidade das conexões do Centro de Operações de Segurança.
- 6.5.5.2. Ambas as conexões digitais devem ter velocidade de upload e download mínima de 10 (dez) Mbps, serem contratadas de operadoras e rotas distintas, e devem ser utilizadas única e exclusivamente para prestação dos serviços presentes no Termo de Referência.
- 6.5.5.3. Especificamente para o tipo de conexão digital internet, necessariamente precisará ter IP dedicado, e não serão aceitos contratos com linksxDSL (executada a tecnologia HDSL). Também, a fim de garantir a disponibilidade da conexão, deverá a CONTRATADA garantir que tal conexão esteja protegida contra-ataques de DDoS - do inglês Distributed Denial of Service.
- 6.5.5.4. É de responsabilidade da CONTRATADA a contratação e os custos relativos ao fornecimento dos links de internet junto às operadoras, durante todo o período de vigência do contrato.
- 6.5.5.5. A fim de garantir a segurança do tráfego bidirecional entre a CONTRATANTE e o Centro de Operações de Segurança da CONTRATADA, ambas as conexões devem ser criptografadas. Ou seja, a CONTRATADA deverá estabelecer duas VPN's - do Inglês Virtual Private Network, do tipo Site To Site, para o Centro de Operações de Segurança.
- 6.5.5.6. A fim de garantir a segurança entre a CONTRATANTE e os Centro de Operações de Segurança da CONTRATADA, não será permitido Centro de Operações de Segurança terceirizado ou consórcio de CONTRATANTES. A CONTRATADA deve ter e manter Centro de Operações de Segurança próprio.
- 6.5.5.7. Por outro lado, a CONTRATADA deve revogar todas as credenciais relacionadas a soluções de sua responsabilidade, empregadas na prestação de serviços para a CONTRATANTE,

bem como solicitar tais revogações à CONTRATANTE, para soluções de responsabilidade da CONTRATADA, no mesmo dia do encerramento das atividades.

- 6.5.5.8. Tais exigências visam proteger o CONTRATANTE contra o uso indevido de informações sob sua custódia, por parte de profissional da CONTRATADA, assim como estão em conformidade com boas práticas de gestão e governança de TI.

6.5.6. DO CENTRO DE OPERAÇÕES DE CIBERSEGURANÇA - CSOC (CYBER SECURITY OPERATION CENTER)

- 6.5.6.1. Os SERVIÇOS GERENCIADOS DE SEGURANÇA devem ser executados por meio de ao menos 01 (um) Centro de Operações de Segurança da CONTRATADA, devendo estar situado obrigatoriamente no Brasil.

6.6. O CSOC deve atender os requisitos mínimos, a saber:

- 6.6.1. Utilizar sistema de gerenciamento de CFTV, que viabilizem o rastreamento de pessoas dentro do ambiente da CONTRATADA e cujas imagens possam ser recuperadas;
- 6.6.2. Filmar toda a área, mantendo as imagens armazenadas por, no mínimo, 90 (noventa) dias;
- 6.6.3. Efetuar registro de entrada e saída dos visitantes, com identificação individual em todos os acessos ao CSOC;
- 6.6.4. Possuir solução de monitoramento de disponibilidade e desempenho.
- 6.6.5. O perímetro físico do CSOC deve ser equipado com sensor de intrusão e alarmes contra acesso indevido;
- 6.6.6. Ser vigiado de forma ininterrupta em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano;
- 6.6.7. Ter controle de acesso físico com pelo menos 2 (dois) dos seguintes fatores de autenticação, a saber: cartão de identificação magnético, biometria de leitura de digital, reconhecimento facial e análise de retina;
- 6.6.8. Funcionar em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano;
- 6.6.9. Possuir registro de entrada e saída de pessoas, mantido por, pelo menos, 90 dias.
- 6.6.10. Possuir sistemas redundantes de alimentação de energia.
- 6.6.11. Para o caso de CSOC que utilize datacenter próprio, possuir estrutura de armazenamento de dados que permita a manutenção dos registros dos eventos relacionados aos serviços contratados por, no mínimo, o prazo do contrato.

- 6.6.12. Ser configurado de forma que a falha de um dos equipamentos isoladamente NÃO interrompa a prestação dos serviços;
 - 6.6.13. Ter sistema de provimento ininterrupto de energia elétrica, composto por grupo gerador e UPSs do inglês Uninterruptible Power Supply, para garantir a transição entre o fornecimento normal da energia e o grupo gerador;
 - 6.6.14. Para o caso de CSOC que utilize datacenter próprio, ter componentes de segurança necessários para garantir a preservação dos dados em casos de incêndio e execução de plano de recuperação de catástrofes;
 - 6.6.15. Deverá possuir processos implementados baseados na norma ABNT NBR ISO/IEC 27001.
- 6.7. Para o caso de CSOC que utilize datacenter próprio, as infraestruturas de datacenter devem estar situadas fora dos ambientes de CSOC, e devem obrigatoriamente atender aos requisitos técnicos elencados, a saber:**
- 6.7.1. Estrutura física dedicada e construída com a finalidade exclusiva de prestação de serviços de hospedagem de aplicações e equipamentos, de modo a garantir um ambiente seguro e controlado, ou seja, não poderá possuir instalações hidráulicas na infraestrutura do Data Center;
 - 6.7.2. Todos os equipamentos envolvidos na solução a ser disponibilizada deverão possuir fontes redundantes;
 - 6.7.3. Deverá possuir área de estacionamento livre e privado, com acesso seguro para desembarque e manuseio de equipamentos com vigilância armada;
 - 6.7.4. Deverá possuir guarita com segurança armada em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano. A guarita de segurança deverá estar fora do prédio de Data Center, criando-se uma barreira física ao acesso do Data Center, ter acesso a todo o sistema de CFTV, inclusive em tempo real, e detecção de intrusos em todas as cercanias onde está localizado o Data Center;
 - 6.7.5. Toda a área do Data Center deve ser desprovida de janelas, básculas ou quaisquer formas de acesso que não através dos controles de acesso;
 - 6.7.6. Garantir a disponibilidade de pessoas dedicadas, treinadas e responsáveis pela segurança de acesso ao prédio e aos equipamentos do ambiente em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano;
 - 6.7.7. Utilizar câmeras digitais de circuito interno de televisão, monitoradas e gerenciadas cujas imagens possam ser posteriormente consultadas por um período mínimo de 90 (noventa) dias, viabilizando o rastreamento de pessoas dentro do ambiente;
 - 6.7.8. As câmeras digitais de circuito interno de televisão deverão cobrir todos os ângulos do túnel frio de forma que não existam quaisquer pontos cegos. A gravação e visualização em tempo

real deverá ser feita em alta-resolução e em cores, com no mínimo 10 frames por segundo. Tais características são necessárias para que seja possível identificação da face daqueles que pretendem adentrar as cercanias do prédio do Data Center;

- 6.7.9. Sistema de detecção e combate a incêndio com uso de sensores de fumaça e fogo distribuídos pela área do Data Center e uso de descarga de gás com efeito supressor de combustão ou redução de oxigênio, ecologicamente aceitável e que não afeta pessoas e equipamentos energizados;
- 6.7.10. Garantir a detecção precoce de gases no ambiente incluindo a área situada sob o piso elevado utilizando detector VESDA, com sistema integrado de alarme monitorado e acompanhado em regime 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano;
- 6.7.11. Possuir sistema integrado aos túneis de ventilação do Data Center, de forma que em havendo o disparo de gás, o fluxo de ar é interrompido para a área do evento garantindo a extinção do incêndio sem afetar demais áreas do Data Center;
- 6.7.12. Em caso de sinistro, o disparo do gás deve ocorrer de forma automática, não havendo necessidade de intervenção humana;
- 6.7.13. O sistema de detecção precoce e combate a incêndio deverá possuir contrato de manutenção contemplando visitas preventivas e testes do sistema com o fabricante do mesmo no mínimo a cada 03 (três) meses;
- 6.7.14. A solução de ar-condicionado deve ser integrada a solução de combate a incêndio para que, em caso de incêndio, os dutos de ventilação sejam automaticamente fechados sem necessidade de intervenção humana;
- 6.7.15. Os equipamentos utilizados para prestação de serviços da CONTRATANTE deverão estar instalados em racks que trabalhem dentro de um sistema de Túnel Frio;
- 6.7.16. A climatização deverá ser composta por, no mínimo, segurança N+1 de unidades evaporadoras e, no mínimo, segurança N+1 de condensadoras externas ao edifício, interligadas por tubos de cobre isolados adequadamente;
- 6.7.17. A climatização não deverá fazer troca de ar atmosférico. Tanto a sala de servidores quanto a sala de refrigeração deverão ser fechadas para que variações de temperatura, umidade e outros contaminantes não afetem os equipamentos dentro do Data Center;
- 6.7.18. Estar equipada com subestação elétrica própria e projetada para operar em média ou alta tensão, para atendimento aos requisitos de potência e alimentação elétrica adequadas e exclusivos para o Data Center;
- 6.7.19. Os sistemas devem ser equipados e protegidos por Nobreaks, bancos de baterias e geradores que funcionam automaticamente no caso de queda do fornecimento comercial;

- 6.7.20. Cada Nobreak deve possuir capacidade suficiente em regime N+1 para suportar todas as atividades do Data Center, incluindo as atividades previstas por este termo de referência;
- 6.7.21. Os nobreaks que atendem aos circuitos redundantes devem operar em regime Standalone, de maneira que os Nobreaks sejam completamente independentes entre si e sem risco de que a falha do primeiro se propague para o segundo;
- 6.7.22. O Data Center deve possuir sistema de geração elétrica à diesel próprio e redundante, que mantenha o ambiente em pleno funcionamento, durante todo o período de eventual corte de energia pela concessionária;
- 6.7.23. A autonomia do sistema de geração elétrica a diesel (grupo gerador) deverá ser de no mínimo 48 (quarenta e oito) horas sem reabastecimento de combustível.
- 6.7.24. Os geradores devem ser capazes de ser acionados para proteger o Data Center automaticamente não apenas em eventos de falta de energia, mas também quando algum parâmetro da concessionária estiver fora das especificações (frequência, tensão etc.);
- 6.7.25. No retorno da alimentação da concessionária, os grupos geradores devem ser capazes de sincronizarem sua alimentação e fazer a retirada da carga em rampa para evitar oscilações elétricas dentro do Data Center;
- 6.7.26. Os geradores e Nobreaks devem possuir contrato de manutenção contemplando visitas preventivas e testes do sistema com o fabricante dos mesmos com periodicidade mínima 1(uma) vez por mês;
- 6.7.27. O prédio da CONTRATADA deve atender a norma NBR 5410 para proteção de surto em todas as zonas.
- 6.7.28. Deve ser um sistema autônomo (AS) em relação à Internet por cadastro próprio, ou seja, possuir seus próprios blocos de IPv4, IPv6 e seu registro individual de ASN.
- 6.7.29. deverá possuir Solução Anti-DDoS, implementando proteção contra-ataques coordenados provenientes de múltiplos sistemas (comprometidos) e distribuídos geograficamente com o intuito de gerar indisponibilidade dos serviços da CONTRATANTE através do esgotamento dos recursos.
- 6.7.30. Deverá ser fornecido o hardware que suporte todas as soluções presentes no Termo de Referência.
- 6.7.31. Possuir ambiente dedicado único e exclusivo para laboratório, onde seja possível reproduzir os incidentes e problemas da CONTRATANTE, sem que haja impacto na operação do Centro de Operações de Segurança e/ou da própria CONTRATANTE;
- 6.7.32. Possuir no Centro de Operações de Segurança processos consistentes e objetivos de monitoramento e detecção de ameaças, gestão de dispositivos, gestão de incidentes, inteligência de ameaças, investigação de ameaças e gestão de conformidade de segurança.

- 6.7.33. Possuir nativamente solução de SecOps para gerenciamento de incidentes de segurança da informação.
- 6.7.34. Deverá possuir processos implementados que garantam o cumprimento das normas e Lei Geral de Proteção de Dados. Tal exigência visa garantir controles rígidos e auditáveis de acesso físico e lógico às informações e monitoramento, além de comprovadamente contar com um comitê responsável pelos controles e adequações;

7. CONDIÇÕES GERAIS PARA PRESTAÇÃO DOS SERVIÇOS

7.1. Independentemente do grupo de serviço especificado, todas as soluções e/ou ferramentas utilizadas para prestação do serviço deverão obrigatoriamente seguir os requisitos, a saber:

- 7.1.1. Deverá ser obrigatoriamente de propriedade da CONTRATADA ou licenciada para a CONTRATADA, não podendo ser do tipo *Open Source* (software livre).
- 7.1.2. Deverá ser prestado por meio de solução provida através da nuvem do fabricante ou da CONTRATADA.
- 7.1.3. Deve englobar o fornecimento de *Hardwares* e de *Softwares* necessários à execução dos serviços contratados durante o prazo de vigência do contrato, incluindo garantia, manutenção, atualização dos produtos e monitoramento de segurança em regime de 24 (vinte quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano;
- 7.1.4. Os softwares ofertados devem ser instalados e atualizados em sua versão mais estável e estar cobertos por contratos de suporte e atualização de versão do fabricante durante a vigência do respectivo item de serviço. Da mesma maneira, os equipamentos fornecidos para a prestação dos serviços devem estar cobertos por contratos de garantia do fabricante;
- 7.1.5. O conjunto de requisitos especificados para cada serviço pode ser atendido por meio de composição com outros equipamentos ou softwares utilizados no atendimento aos demais itens, de maneira integrada, desde que não implique alteração da topologia de rede ou na exposição de ativos a riscos de segurança da informação, em termos de integridade, confidencialidade ou disponibilidade.

7.2. EQUIPE DE INTELIGENCIA DE AMEAÇAS

- 7.2.1. A contratada deverá contar com uma equipe de inteligência de ameaças dedicada a identificar as intenções, capacidades e, prioritariamente, as oportunidades usadas pelos criminosos através da coleta, normalização, correlação e análise de dados, transformando-os em inteligência e entregando ao CONTRATANTE relatórios periódicos, apresentando dados de mercado e o atual cenário do ambiente do CLIENTE.
- 7.2.2. Esses dados poderão ser utilizados para melhora na proteção, seja na atuação direta com a equipe de *Hunting* em novos casos de uso ou mantendo o time da CONTRATANTE informados, através de Boletins de Ameaças.

- 7.2.3. A CONTRATADA deverá possuir célula que entregue informações através de fontes de inteligências abertas e/ou próprias, compartilhando informações de inteligência através do MISP (*Malware Information Sharing Platform*), executando também a gestão dele através da equipe local, bem gerindo a integração entre o MISP da CONTRATANTE como da CONTRATADA.
- 7.2.4. A plataforma deverá ter capacidade de identificar vulnerabilidades em, no máximo, um dia após o surgimento desta, executar o correlacionamento com o inventário informado pela CONTRATANTE e informar via evento no MISP sobre os sistemas vulneráveis.
- 7.2.5. A CONTRATADA deverá possuir plataforma de inteligência que informe IoCs (Indicadores de Comprometimento) contendo, no mínimo, *Hashes* de binários maliciosos nos formatos MD5, SHA1, SHA256, *Filename*, domínios maliciosos, URLs maliciosas, bem como IPs maliciosos com geolocalização e pontuação de risco, reduzindo a possibilidade de falso positivo;
- 7.2.6. Deve possuir equipe de *Threat Intelligence* que execute Análise de Superfície, um trabalho que avalia o ambiente na perspectiva de um agente malicioso em busca de eventuais brechas utilizando o *Framework* OSINT (Inteligência de Fontes Abertas) com foco na identificação de superfície de ataque e as possíveis oportunidades na perspectiva de um agente malicioso.
- 7.2.7. Deve executar de forma recorrente a Análise de Superfície, no mínimo trimestralmente, utilizando especialistas de *Cyber Threat Intelligence* na execução de um *Assessment* interno e análise externa utilizando técnicas de OSINT, apresentando informações dos perímetros com objetivo de entregar relatório, apontando de forma prática como tratar cada ponto identificado e apresentar um *Score* qualitativo de maturidade para a CONTRATANTE.

7.3. PORTAL DE INDICADORES DE SERVIÇO

- 7.3.1. O portal de indicadores deverá ser disponibilizado à CONTRATANTE e contemplar, no mínimo, os requisitos abaixo:
- 7.3.2. A CONTRATADA deverá disponibilizar um sistema em modelo SaaS (do inglês *Software As Service*), denominado portal de indicadores, para consolidação dos dados gerados pelas soluções que compõem o objeto.
- 7.3.3. O portal deverá estar acessível à CONTRATADA via *Internet*, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, e 365 (trezentos e sessenta e cinco) dias por ano, de maneira segura utilizando protocolo de criptografia SSL.
- 7.3.4. A CONTRATANTE terá direito a criação de usuários ilimitados com a função de criação de perfis para cada usuário, disponibilizando assim visões diferentes para cada nível de acesso.
- 7.3.5. Deverá disponibilizar para os usuários da CONTRATANTE a função de mudança de visão gráfica a critério de cada usuário. Isso quer dizer que apesar de um gráfico estar disposto em modelo de barras, caso o usuário identifique uma melhor visualização do modelo gráfico em forma de pizza, o sistema deve oferecer tal funcionalidade ou opção.

7.3.6. O portal ainda deverá disponibilizar os seguintes modelos gráficos para os usuários:

- a) Gráfico do tipo Pizza;
- b) Gráfico do tipo Barra;
- c) Gráfico do tipo linha;
- d) Gráfico do tipo área;
- e) Gráfico do tipo funil;
- f) Gráfico do tipo bolha.

7.3.7. INDICADORES DE RISCO – KRI:

- 7.3.7.1. Deverá ser exibido no portal a quantidade de Vulnerabilidades que estavam presentes na última auditoria realizada através de gráfico(s) com separação dos tipos/quantidades com a opção de “Drill Down”, possibilitando assim visualização de forma mais detalhada das vulnerabilidades listadas;
- 7.3.7.2. O portal deverá possuir recurso para filtrar apenas as vulnerabilidades relevantes, excluindo as de severidade média e/ou baixa.

7.3.8. INDICADORES DE META E PERFORMANCE – KGI e KPI:

- 7.3.8.1. O portal de indicadores deverá possuir relatório gráfico indicando tempo médio dos atendimentos dos incidentes por fase de Análise, contenção, erradicação e recuperação, possibilitando a filtragem por período:
 - 7.3.8.2. Últimos 15 dias;
 - 7.3.8.3. Últimos 30 dias;
 - 7.3.8.4. Últimos 45 dias.
- 7.3.9. Deverá possuir gráfico comparativo entre os primeiros e últimos 15 incidentes analisados dentro de período filtrado, mostrando numa linha de tempo qual foi o incidente com o tempo de atendimento menor, maior e o tempo médio.
- 7.3.10. Deverá ser possível a consulta deste gráfico para cada uma das fases de atendimento (análise, contenção, erradicação e recuperação).

7.4. INDICADORES POR CATEGORIA MITRE ATT&CK:

- 7.4.1. O Portal de indicadores deverá possuir gráfico que separe e classifique os incidentes de acordo com as categorias existentes na base de conhecimento do MITRE ATT&CK, sendo elas no mínimo:
 - a) Initial Access;
 - b) Execution;
 - c) Persistence;
 - d) Privilege Escalation;

- e) Defense Evasion;
- f) Lateral Movement;
- g) Collection;
- h) Command and Control;
- i) Exfiltration;
- j) Impact.

- 7.4.2. Todos os indicadores exibidos pelo portal, devem possuir a funcionalidade *Drill Down*, para que os usuários possam criar visualizações e filtros dos dados exibidos.
- 7.4.3. Todos os indicadores exibidos pelo portal devem ainda possuir funcionalidade de exibição dos dados gerados do gráfico de maneira tabular, a fim de que seja possível aferir os dados brutos.
- 7.4.4. O portal deve armazenar os dados durante o período mínimo de 1 (um) ano e deverá permitir a criação de filtros por períodos.
- 7.4.5. A qualquer tempo a CONTRATANTE poderá solicitar os dados brutos coletados das soluções que compõem o objeto contratado.
- 7.4.6. Os dados exibidos pelo portal devem representar o ambiente em tempo de execução e de forma automática (*Real Time*).
- 7.4.7. O portal deverá possibilitar customizar limiares dos serviços e eventos para gerar alarmes de acordo com o acordo de nível de serviço definido no presente termo de referência;
- 7.4.8. Deverá prover mecanismo para análise de risco e métricas de disponibilidade através de relatórios e *Dashboards* de todas as soluções que compõem o objeto.

7.5. SERVIÇO DE ACOMPANHAMENTO DE ENTREGAS

- 7.5.1. Deverá ser provido um serviço de acompanhamento de entregas através de reuniões de preferência virtuais para cadência do contrato de forma quinzenal.
- 7.5.2. **Entregável:** Ata de reunião
- 7.5.3. Deverá ser feito o acompanhamento periódico dos indicadores listados no contrato para antecipar desvios e corrigi-los antes que saiam das conformidades exigidas;
- 7.5.4. **Entregável:** Acompanhamento periódico a partir das ferramentas de registro de chamado ou medição (Portal de Indicadores);
- 7.5.5. **Entregável:** Checklist periódico dos entregáveis do projeto, conforme RFP, TR, proposta técnica e afins.
- 7.5.6. Deverá ser feito o acompanhamento do cronograma de faturamento mensal do contrato;
- 7.5.7. Deverá manter a matriz de comunicação atualizada dos dois lados do contrato – quem a

CONTRATADA deve acionar e quem a CONTRATANTE deve acionar em casos específicos ou de escalação.

7.5.8. **Entregável:** Documento formal conforme formato pré-estabelecido.

7.6. SERVIÇO DE CONFORMIDADE DE DESEMPENHO CONTRATUAL

- 7.6.1. Deve ser provido serviço de conformidade de desempenho do contrato no qual deverão ser providas reuniões mensais entre a CONTRATANTE e a CONTRATADA com intuito de validação da satisfação referente aos serviços prestados.
- 7.6.2. Estas reuniões devem servir para identificação das necessidades da CONTRATANTE onde deverão ser apontados problemas recorrentes ou pontuais que estejam impactando a qualidade da execução do contrato.
- 7.6.3. Após essas reuniões deverão ser formulados planos de ações corretivos para cada área/serviço que não esteja cumprindo os padrões de qualidade exigidos no contrato.
- 7.6.4. O serviço deve ser executado por um especialista em resolução de crises ou temas críticos da CONTRATADA que funcione como moderador entre o time de entrega da CONTRATADA com os gestores do contrato da CONTRATANTE.
- 7.6.5. Entende-se como CRISE a atuação que é ou será baseada no desenvolvimento de um plano de ação para temas que gerem ônus imediato à CONTRATANTE, ônus direto e imediato à CONTRATADA, risco de exposição do ambiente da CONTRATANTE, risco de cancelamentos de contratos. Além disso, crises serão tratadas em conjunto com todas as áreas envolvidas, até a finalização do plano de ação de correção.
- 7.6.6. O especialista responsável por este serviço deve atuar também na escalação de temas não críticos do dia a dia do contrato que não estejam sendo respondidos devidamente pela CONTRATADA.
- 7.6.7. Entende-se como ESCALAÇÃO problemas diários da CONTRATANTE em que a tratativa não foi eficaz e efetiva e/ou fora do tempo esperado/acordado, fazendo com que a CONTRATANTE eleve o tema para um nível hierárquico superior da CONTRATADA. Exemplos:
 - 7.6.7.1. Falta de atuação de algum time específico;
 - 7.6.7.2. Falta de resposta à um e-mail, chamado e/ou questionamentos do CONTRATANTE;
 - 7.6.7.3. Falta de solução à um problema sinalizado pelo CONTRATANTE;
 - 7.6.7.4. Chamado em aberto, não atendido dentro do SLA acordado em contrato;
 - 7.6.7.5. Insatisfação da CONTRATANTE sobre um entregável como relatório, boletins, atuação/postura de recursos ou times;

- 7.6.8. Este serviço deverá prover ainda um indicador denominado NPS (Net Promoter Score) que consiga metrificar a satisfação da CONTRATANTE em relação aos serviços prestados que estejam estipulados no contrato. Está métrica deverá seguir os padrões e fórmulas comuns de mercado e deverá ser atualizada e apresentada mensalmente aos gestores do contrato.
- 7.6.9. Em quaisquer mudanças em que a CONTRATADA identifique possíveis impactos no ambiente, e/ou que necessite de alterações de configurações em servidores ou ferramentas que possuam amplo alcance deverão passar pelo processo de aprovação de RDM (Requisição de Mudança) da CONTRATANTE.

8. ESPECIFICAÇÃO DOS SERVIÇOS

8.1. SERVIÇOS DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS E RESPOSTA A INCIDENTES

- 8.1.1. Visa o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados a CONTRATANTE, através de fornecimento de serviços com capacidade de correlacionamento de eventos, para detecção de ameaças direcionadas a CONTRATADA para detecção de comportamento anômalo de serviços, que possam gerar eventos de segurança da informação, aos quais devem ser analisados, podendo estes serem transformados em um incidente de segurança da informação, obedecendo um processo cíclico e rigoroso de gestão de eventos.

8.1.2. SOBRE AS FERRAMENTAS A SEREM UTILIZADAS

- 8.1.2.1. Para execução deste serviço, a CONTRATADA deverá utilizar e ser capaz de fornecer, operar, sustentar e suportar soluções de monitoramento que atendam o descritivo técnico a seguir:
- 8.1.2.2. A plataforma utilizada deverá ter capacidade de operar com volumes massivos de dados em tempo real utilizando algoritmos de aprendizagem de automático de máquina "*Machine Learning*" e deve contar com casos de uso para detectar ameaças avançadas.
- 8.1.2.3. A plataforma deverá possuir as características a seguir:
- 8.1.2.4. Extremamente escalável e tolerante a falhas, capaz de ingerir centenas de terabytes por dia e suportar a retenção de eventos de segurança por longo período.
- 8.1.2.5. Junte-se a eventos ao longo do tempo usando modelos Kill Chain para a análise de eventos de maior risco.
- 8.1.2.6. Permitir o hunting rápido de ameaças por meio da pesquisa em linguagem natural.
- 8.1.2.6.1. A solução deve estar classificada como líder no quadrante mágico de "Security Information and Event Management" pelo menos no último ou penúltimo ano;
- 8.1.2.6.2. A solução deve ter recursos de "Multi-tenant";

- 8.1.2.6.3. Deve ser do tipo Nuvem em Software como um modo de Serviço e ter as certificações SOC 2 TYPE II e ISO 27001.
- 8.1.2.6.4. Deve garantir retenção dos logs conforme arquitetura abaixo:
 - a) 7 dias hot retention;
 - b) 90 dias warm retention;
 - c) 365 dias cold retention.
- 8.1.2.6.5. Deve ter alta disponibilidade e mecanismos de recuperação de desastres;
- 8.1.2.6.6. Deve permitir a filtragem e compressão de dados seletivos em até 90% no ponto de coleta;
- 8.1.2.6.7. Deve permitir o gerenciamento da largura de banda para a transmissão de dados entre os coletores e os servidores de gerenciamento;
- 8.1.2.6.8. Deve executar o armazenamento em cache local e/ou em buffer nos coletores para garantir que nenhum dado seja perdido em trânsito no caso de um problema de rede ou um pico no volume do evento;
- 8.1.2.6.9. Deve oferecer suporte ao mascaramento de dados por meio de controles de acesso granulares baseados em funções, para ofuscar qualquer informação de usuário potencialmente sensível na camada de interface do usuário;
- 8.1.2.6.10. Deve suportar controle de acesso baseado em função granular (RBAC) com suporte a administração delegada, tanto para as funcionalidades na interface do usuário quanto acesso aos dados e configurações;
- 8.1.2.6.11. Deve incluir uma ferramenta de Security Datalake baseada em bigdata em uma arquitetura aberta e escalável e com capacidade de coletar e reter dados por períodos estabelecidos para fins de conformidade e investigação;
- 8.1.2.6.12. Deve ter uma instância de homologação para testes que permita isolar, do ambiente de produção, novas integrações, novos desenvolvimentos de conteúdos e novos analisadores;
- 8.1.2.6.13. A solução deve atender as seguintes características:
 - 8.1.2.6.13.1. Deve oferecer suporte a integração com mais de 500 fontes de eventos usando métodos de syslog, formatos de log estruturados (CEF, LEEF, MEF, JSON, XML), arquivos, bancos de dados (conexão JDBC), conexão API (AWS, Azure, Box, Crowdstrike, Google Report, Netskope, SVN, Salesforce, Splunk, QRadar, Netwitness, Office 365, Okta, Proofpoint, Sumologic, Workday, entre outros), WMI, consultas

LDAP/LDAPS, dados e fluxo (Netflow, sFlow, jFlow), Hadoop, Registros não estruturados (Regex), agentes de terceiros (snare);

- 8.1.2.6.14. Deve permitir a integração com diferentes tipos de fontes de dados, como dados de identidade, logs de atividades / transações, logs de eventos de segurança, fluxos de rede, log de aplicativos / plataformas de nuvem, permissões de acesso, fontes de inteligência de ameaças, dados não estruturados e metadados de ativos;
- 8.1.2.6.15. Deve permitir conexão a sistemas externos de gerenciamento de identidade, como Active Directory / LDAP ou soluções de IAM (gestão de identidade), como Aveksa/Sailpoint, sistemas de RH, como Peoplesoft/Workday, para realizar o enriquecimento contextual de eventos adicionando identidade do usuário;
- 8.1.2.6.16. Deve ser capaz de se conectar nativamente através de APIs ou outros meios com serviços em nuvem como Salesforce, Amazon Web Services S3 e Cloudtrail, BOX, Microsoft Azure, Office 365, Google Apps, Google Cloud, Netskop, ServiceNow, entre outros.
- 8.1.2.6.17. Deve ter uma interface de usuário que permita modificar conectores, analisadores (parsers) existentes ou construir novos analisadores (parsers) na mesma interface de usuário;
- 8.1.2.6.18. Deve ter conectores, analisadores (parsers) pré-configurados, prontos para uso, mas que possam ser modificados conforme necessário. A análise, normalização e categorização dos coletores devem ser totalmente personalizáveis na interface do usuário.
- 8.1.2.6.19. Deve ter uma API RESTful de serviços para integração bidirecional com outras tecnologias;
- 8.1.2.6.20. Deve fornecer integração com pelo menos 5 fontes de inteligência de ameaças incluídas no valor do serviço ofertado;
- 8.1.2.6.21. Deve realizar o enriquecimento dos eventos com dados contextuais sobre eventos no momento da captura e ingestão de dados adicionando aos eventos:
 - a) Identidade do usuário;
 - b) Contexto de negócios;
 - c) Metadados de ativos;
 - d) Informações de rede;
 - e) Localização Geográfica;
 - f) Dados de inteligência de ameaças;

- 8.1.2.6.22. Deve enriquecer eventos em tempo real com contexto de usuário e entidade. Os dados ricos podem fornecer atributos de contexto que podem ser usados para perfis comportamentais, comparações de pares, pesquisas e investigações;
- 8.1.2.6.23. Deve detectar ameaças cibernéticas e internas avançadas (insider threat) usando aprendizado de máquina para criar perfis e linhas de base de comportamento de usuários e entidades;
- 8.1.2.6.24. Deve ter conteúdo pré-empacotado de casos de uso e modelos de ameaças prontos para uso para detecção avançada de ameaças, como:
- a) Detecção de ameaças internas (insider threat) utilizando técnicas de aprendizagem de máquina;
 - b) Detecção de ameaças cibernéticas (cyber threat) utilizando técnicas de aprendizagem de máquina;
 - c) Detecção de ameaças na nuvem (cloud threat) utilizando técnicas de aprendizagem de máquina;
- 8.1.2.6.25. Deve fornecer recursos abrangentes para modelar e ajustar a pontuação de risco com base no perfil do usuário e/ou entidade, gravidade da ameaça e sequência/combinção de eventos que ocorrem durante um período;
- 8.1.2.6.26. Deve permitir a modelagem de risco a partir da interface do usuário de acordo com as prioridades da organização;
- 8.1.2.6.27. Deve ter modelos de ameaças que permitam agrupar eventos realizados por um usuário ou entidade que duram dias, semanas, meses e assim por diante. Essas atividades devem ser exibidas como uma cadeia de eliminação com cada evento categorizado em estágios predefinidos.
- 8.1.2.6.28. Deve ter algoritmos preditivos para identificar usuários de risco (por exemplo, usuários prestes a deixar a organização);
- 8.1.2.6.29. Deve fornecer análises para diferentes tipos de anomalias, como relacionadas ao tempo, volume de transferência de dados, origem do evento relacionado, destino do evento relacionado, anomalias por usuário e grupo de pares, anomalias relacionadas a localização geográfica / velocidade terrestre, bem como rastrear usuários ou outras entidades nas listas de observação;
- 8.1.2.6.30. Deve ter algoritmos de aprendizagem não supervisionados para analisar eventos atuais e históricos e determinar associações, para estabelecer padrões de comportamento da atividade do usuário em cada fonte de evento por dia, semana, mês, hora do dia e dia da semana. Qualquer desvio do padrão regular deve ser marcado como uma anomalia;

- 8.1.2.6.31. Deve ter algoritmos de aprendizagem supervisionados para detectar ameaças de malware avançadas, como DGA, ataques de phishing/spam e muito mais;
- 8.1.2.6.32. Deve ter técnicas de análise baseadas pares para detectar usuários que estão começando a se comportar de maneira diferente dos pares, traçando o perfil do comportamento de diferentes usuários no grupo de pares e, em seguida, comparando as transações do usuário com a dos pares;
- 8.1.2.6.33. Deve haver técnicas de análise de raridade de eventos pelas quais atividades suspeitas que não foram vistas antes possam ser identificadas;
- 8.1.2.6.34. Deve ter técnicas de análise de comportamento por enumeração que permita criar linhas de base de eventos do mesmo tipo e procurar qualquer desvio do normal;
- 8.1.2.6.35. Deve ter técnicas de análise de tráfego para identificar padrões de beaconing, agentes de usuários incomuns, conexões com URLs incomuns, conexões com domínios DGA, etc;
- 8.1.2.6.36. Deve fornecer a capacidade de definir políticas baseadas em regras para detectar ameaças conhecidas. Essas ameaças conhecidas devem ser usadas como intensificadores de risco e combinadas com as verificações “não assinadas” nos modelos de ameaças;
- 8.1.2.6.37. Deve haver modelagem de ameaças que permita a identificação de ameaças compostas, que se observadas isoladamente podem ser de baixo risco, porém, quando combinadas, são indicativas de um evento de alto risco;
- 8.1.2.6.38. Deve reduzir o número de falsos positivos aplicando recursos avançados de aprendizado de máquina para aprender o que é normal e o que não é normal no ambiente monitorado;
- 8.1.2.6.39. Deve ter relatórios de ameaças que forneçam visibilidade da postura de segurança cibernética. Por exemplo: usuários de alto risco, ativos de alto risco, principais ameaças, principais IPs maliciosas, etc;
- 8.1.2.6.40. Deve ter relatórios que forneçam visibilidade sobre as operações de segurança. Por exemplo, para dispositivos VPN, os relatórios devem incluir as melhores sessões de VPN por duração, os principais eventos de saída de dados, a distribuição dos eventos de login por geografia, as principais tentativas de login com falha e assim por diante;
- 8.1.2.6.41. Deve ter relatórios de conformidade alinhados com requisitos de conformidade específicos, como PCI, SOX, HIPPA, GDPR, ISO27002, etc;
- 8.1.2.6.42. Deve ter relatórios de resumo executivo de violações, incidentes e operações;
- 8.1.2.6.43. Deve ter relatórios sobre a atividade do usuário;

- 8.1.2.6.44. Deve permitir que os dados sejam exibidos com diferentes tipos de gráficos: gráfico de linhas, gráfico de barras, gráfico de pizza, mapa geográfico, tabelas, gráfico empilhados, gráfico N principais, gráficos de bolhas, gráficos de relacionamento de origem e destino;
- 8.1.2.6.45. Deve permitir a visualização de dados através de links que permitam vincular qualquer conjunto de atributos e visualização a relação entre eles;
- 8.1.2.6.46. O serviço deve possuir solução para análise de artefatos maliciosos que minimamente contemple as funcionalidades a seguir:
- a) Analisar mais de 1000 indicadores comportamentais de um artefato;
 - b) Realizar análise estatística e dinâmica para avaliar se o artefato é malicioso ou não;
 - c) Deve suportar a análise dos artefatos BAT, CHM, DLL, ISO, HTA, HWP, JAR, JS, JSE, JTD, LNK, MSI, MHTML, documentos do Microsoft Office, EXE, PE32, PDF, VBE, URLs, WSF, XML e ZIP;

8.1.3. PROCESSOS A SEREM APLICADOS

8.1.3.1. PROCESSO DE MONITORAMENTO, DETECÇÃO E RESPOSTA

- 8.1.3.1.1. A CONTRATADA será responsável por implantar, operar e suportar toda a plataforma ofertada;
- 8.1.3.1.2. A fim de balizar todo o processo de monitoramento de ataques cibernéticos da CONTRATANTE, e influenciado pelos principais frameworks de boas práticas de serviços de segurança da informação, deverá ser desenhado/revisado em conjunto com a CONTRATANTE, o processo de resposta a incidentes focado em cibersegurança escopo desse contrato, que seja aderente as características específicas do ambiente da CONTRATANTE.
- 8.1.3.1.3. Após a definição/revisão e escrita da política de respostas a incidentes de cibersegurança, para início da implementação dos processos, deverá haver o aceite formal da CONTRATANTE.
- 8.1.3.1.4. É sabido que para o sucesso de um monitoramento de ataques cibernético, a primeira definição se deve a que tipo de ocorrência de eventos de segurança, se deseja detectar e tomar algum tipo de ação, logo será de responsabilidade da CONTRATADA como primeiro passo deste processo, a definição de linha de base de eventos monitorados.
- 8.1.3.1.5. Tal definição de linha de base de eventos de segurança monitorados, não deve ser tomada de forma unilateral pela CONTRATADA. A CONTRATANTE deverá

participar ativamente no processo de construção de forma consultiva. Porém, se ratifica que é de responsabilidade da CONTRATADA a definição, e colocar em operação tal linha de base.

- 8.1.3.1.6. Espera-se que a linha de base de eventos de segurança monitorados, seja revista de forma mensal, contudo, não se limitando a este tempo, pois todos os dias novos ataques são projetados no mundo, e se espera que a CONTRATADA tome ciência destes ataques, e por sua vez atualize a linha de base, para que em um cenário onde estes novos ataques sejam direcionados a CONTRATANTE, sejam detectados através dos serviços em questão.
- 8.1.3.1.7. O produto de um evento é a correlação dos logs gerados pelos itens de configurações do parque da CONTRATANTE. Uma vez definida a linha de base de eventos, será também de responsabilidade da CONTRATADA avaliar se todos os insumos para a correta geração do evento, estão sendo enviados corretamente para a ferramenta.
- 8.1.3.1.8. Caso a CONTRATADA identifique a ausência dos insumos (eventos) a ser gerado por um item de configuração, será de responsabilidade da CONTRATADA a correção e/ou habilitação de tal insumo dos itens de configuração descritos no tópico AMBIENTE TECNOLÓGICO DA CONTRATANTE (HARDWARE E SOFTWARE). Caso o item de configuração não pertencer ao objeto contratado, porém necessário para a correta geração do evento, deverá a CONTRATADA solicitar a CONTRATANTE a correção e/ou habilitação de tal insumo no item de configuração em questão.
- 8.1.3.1.9. Dar-se-á então o passo de classificação do evento, também de responsabilidade da CONTRATADA. O grupo de monitoramento de ataques da CONTRATADA deve focar as ações nos eventos que são significativos. Logo, tal grupo deve analisar todos os eventos apresentados, classificando-os nos seguintes grupos, a saber:
 - 8.1.3.1.9.1. Eventos de Informação: Estes eventos não requerem qualquer ação. São usados para fazer verificação de funcionalidade dos itens de configuração de segurança. Ou seja, tem por objetivo puro e simples, identificar se as ferramentas e soluções estão funcionando dentro do esperado. Estes eventos são também úteis para gerar estatísticas como, por exemplo, porcentagem de hosts com a última vacina de antivírus do dia.
 - 8.1.3.1.9.2. Eventos de Aviso: Este grupo de eventos deve ser utilizado quando existe algum comportamento anômalo, se comparado a linha de base de operação padrão do ambiente (serviço ou solução), porém, ainda não gerou algum tipo de impacto ao ambiente (serviço ou solução) da CONTRATANTE, como por exemplo fictício: É esperado que exista 1.000 (mil) ataques do tipo port scan bloqueados pelo firewall, porém, na última hora, este número passou para 10.000 (dez mil) ataques, todavia,

o firewall ainda continua bloqueando sem que haja degradação da performance do ambiente (serviço, tráfego e/ou solução).

- 8.1.3.1.9.3. Eventos de Exceção: Estes eventos são aqueles que sugere que os pilares de segurança da informação (confidencialidade, integridade e conformidade), foram impactados como, por exemplo: Uma infecção gerada por um malware do tipo ransomware, onde a mesma não tenha sido bloqueada pela solução de antivírus da CONTRATANTE. Este é o único tipo de evento que pode iniciar o processo de resposta a incidente de segurança, descrito no tópico, do presente termo de referência.
- 8.1.3.1.9.4. Uma vez classificado o evento, se inicia o passo de resposta ao mesmo, que também é de responsabilidade da CONTRATADA. As respostas a serem dadas a cada tipo de incidentes, serão baseadas na política de resposta a incidentes escrita previamente conforme descrito no presente termo.
- 8.1.3.1.9.5. Durante a fase de escrita e/ou definição dos processos a serem seguidos, deverá ser informado quais os respectivos tipos de ações para no mínimo os seguintes tipos de eventos:
- 8.1.3.1.9.6. Informacional;
- 8.1.3.1.9.7. Aviso;
- 8.1.3.1.9.8. Exceção;
- 8.1.3.1.10. Importante ressaltar que todo o processo de tratamento do evento, independente de qual fase e/ou status, deve ser registrado no módulo de tratamento de eventos da ferramenta. Também é responsabilidade da CONTRATADA a segurança dos eventos, e fica expressamente proibido a remoção de qualquer evento, independentemente de sua classificação e fase de tratamento, sem a autorização da contratante.
- 8.1.3.1.11. Deverá em conjunto com a CONTRATANTE, ser criado playbooks de resposta a incidentes.

8.1.4. GRUPO TÉCNICO DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS

- 8.1.4.1. Através do seu centro de operação de segurança, a CONTRATADA deverá manter uma torre de operação denominada GRUPO DE MONITORAMENTO DE ATAQUES, com objetivo e foco de trabalhar no processo de monitoramento de ataques cibernéticos.
- 8.1.4.2. Este grupo deverá ser exclusivo para trabalhar no serviço em questão, não podem os profissionais pertencentes a este grupo serem compartilhados e/ou atuarem, com os demais serviços descritos no objeto do presente termo de referência.
- 8.1.4.3. Todos os profissionais que integram GRUPO DE MONITORAMENTO DE ATAQUES, devem

obrigatoriamente compor o quadro permanente de colaboradores da CONTRATADA em regime de trabalho CLT (Consolidação das Leis do Trabalho) ou contrato de prestação de serviços firmados diretamente entre esses profissionais e a CONTRATADA, sendo proibida a terceirização ou subcontratação de tal serviço.

8.1.4.4. Além dos profissionais que deverão ficar dedicados ao contrato conforme informado previamente no presente termo de referência o dimensionamento é de responsabilidade da CONTRATADA quantificar o número adequado de profissionais para a entrega de tal serviço, sem que haja impacto no acordo de nível de serviço estabelecido no tópico ACORDO DE NÍVEIS DE SERVIÇO do presente termo de referência.

8.1.4.5. A fim de garantir que os profissionais envolvidos tenham conhecimento e habilidade para executar o processo de monitoramento de ataques cibernéticos da CONTRATANTE, a CONTRATADA deverá, obrigatoriamente, compor o GRUPO DE MONITORAMENTO DE ATAQUES, com ao menos 01 (um) perfil de cada profissional que segue descrito abaixo:

Perfis	Certificações	Descrição
Analista de Segurança I	- CompTIA Security+ - CompTIA CySA+ e/ou Certified Ethical Hacker - Certificação em pelo menos uma das soluções escolhidas para atender o tópico SOBRE AS FERRAMENTAS A SEREM UTILIZADAS	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.
Analista de Segurança II	- CompTIA Security+ e/ou CompTIA CySA+ e/ou - Certified Ethical Hacker	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e

		soluções de SIEM e ATD. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.

Tabela 2 - Certificações e qualificações do Grupo de Monitoramento de Ataques

8.1.4.6. Não existe restrição ou limite para acúmulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos no GRUPO DE MONITORAMENTO DE ATAQUES, porém, conforme já foi mencionado neste termo de referência, este(s) deve(m) compor única e exclusivamente o time denominado GRUPO DE MONITORAMENTO DE ATAQUES.

8.1.4.7. ENTREGAS A SEREM REALIZADAS

8.1.4.7.1. Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, o CONTRATANTE definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue de forma on line e em tempo de execução, através do portal de indicadores descrito no tópico de condições gerais para prestação do serviço deste termo de referência, a saber:

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Quantitativo de eventos correlacionados	Soma de eventos correlacionados	Eventos correlacionados	Eventos correlacionados	Número total de eventos correlacionados
Quantitativo de incidentes abertos	Soma de incidentes abertos	Incidentes abertos	Incidentes	Número total de incidentes abertos
Quantitativo de solicitações por grupo de tecnologia	Soma de solicitações relacionadas aos grupos de tecnologia	Solicitações relacionadas aos grupos de tecnologia	Solicitações	Número total de solicitações relacionadas por grupo de tecnologia
Quantitativo de regras de correlacionamento	Soma do número de regras de correlacionamento	Regras de correlacionamento	Regras de correlacionamento	Número total de regras de correlacionamento
TOP 10 – Regras de correlacionamento	Soma do número de eventos correlacionados por regra de correlacionamento	Eventos correlacionados	Regra de correlacionamento	TOP 10 do número de eventos correlacionados por regra de correlacionamento
TOP 10 – IP de destino de regras de correlacionamento	Soma do número de eventos correlacionados por IP de destino	Eventos correlacionados por IP de destino	IP de destino	TOP do número de eventos correlacionados por IP de destino

TOP 10 – Regras de correlacionamento por país de origem	Soma do número de eventos correlacionados por país de origem	Eventos correlacionados por país de origem	País de origem	TOP do número de eventos correlacionados por país de origem
TOP 10 – Tipos de ataques	Soma do número de ataques correlacionados por tipo de ataque	Eventos correlacionados por ataque	Ataques	TOP 10 por tipo de ataque

Tabela 3 - Indicadores Estratégicos de Monitoramento de Ataques Cibernéticos

9. SERVIÇO DE GESTÃO DE VULNERABILIDADES PARA 300 (TREZENTOS) ATIVOS

9.1. Tem por objetivo de forma proativa e recorrente, identificar possíveis vulnerabilidades de segurança da informação, na infraestrutura e aplicações do CONTRATANTE, identificando proativamente as vulnerabilidades de aplicações que seriam vetores de ataques, e tornando-as elegíveis de blindagem contra a exploração das vulnerabilidades identificadas afim de evitar que ataques cibernéticos direcionados ao CONTRATANTE, obtenha sucesso explorando tais vulnerabilidades já conhecidas.

9.2. SOBRE AS FERRAMENTAS A SEREM UTILIZADAS

9.2.1. ESPECIFICAÇÕES GERAIS

- 9.2.1.1. A solução deve realizar varreduras (*Scans*) de vulnerabilidades, avaliação de configuração e conformidade (*Baseline e Compliance*);
- 9.2.1.2. A solução deve possuir recurso de varredura ativa, onde o *Scanner* comunica-se com os alvos (ativos) através da rede;
- 9.2.1.3. A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT;
- 9.2.1.4. A solução deve ser licenciada pelo número de endereços IP ou dispositivos (*Assets*);
- 9.2.1.5. A solução deve fornecer um modelo de armazenamento integrado que não dependa de um banco de dados externos ou de terceiros;
- 9.2.1.6. Caso a solução dependa de banco de dados de terceiros, todas as licenças deverão ser fornecidas pela CONTRATADA.
- 9.2.1.7. A solução deverá suportar API (*Application Programming Interface*) baseada em REST (*Representational State Transfer*) para automação de processos e integração com aplicações terceiras.
- 9.2.1.8. A solução deve possuir integração via API no mínimo para as seguintes linguagens: *Python, Powershell, Ruby, Javascript, Java, Swift e PHP*;
- 9.2.1.9. A solução deve possuir métodos de consulta via API e envio, tais como: HTTP METHOD (POST, GET, PUT AND DELETE);

- 9.2.1.10. A solução deve incluir a opção para agentes instalados e licenciados em estações de trabalho e servidores para varredura diretamente no sistema operacional;
- 9.2.1.11. Tais agentes devem ser gerenciados pela mesma interface/console da plataforma de gestão de vulnerabilidades;
- 9.2.1.12. A solução deve permitir o agrupamento de *Scanners* para facilitar o gerenciamento e aplicação de políticas;
- 9.2.1.13. A solução deve realizar a varredura tanto de dispositivos na rede interna, dispositivos expostos a demais redes externas, tanto quanto dispositivos em nuvens públicas como Azure, AWS ou GCP;
- 9.2.1.14. O escaneamento para os dispositivos expostos deve ser realizados através de SCANS (ENGINE) do próprio fabricante alocados no Brasil;
- 9.2.1.15. Os Scanners e sensores agentes deverão ser gerenciados por uma única plataforma, de maneira centralizada;
- 9.2.1.16. O acesso a console de gerenciamento deve ser fornecida para pelo menos 10 usuários simultâneos;
- 9.2.1.17. A solução deve ser capaz de se integrar e disponibilizar insumos para soluções de correlação de eventos externa (SIEM);
- 9.2.1.18. A solução deve apresentar, para cada vulnerabilidade encontrada, a descrição e passos que devem ser tomados para correção;
- 9.2.1.19. A solução deve apresentar, para cada vulnerabilidade encontrada, evidências da vulnerabilidade através de saídas das verificações (Outputs);
- 9.2.1.20. A solução deve fornecer controle de acesso baseado em função (RBAC- Role Based Access Control) para controlar o acesso do usuário a conjuntos de dados e funcionalidades;
- 9.2.1.21. A solução deve ser capaz de definir e gerenciar grupos de usuários, incluindo limitação de funções de varreduras e acesso a relatórios e Dashboards;
- 9.2.1.22. A solução deve ter a capacidade de excluir determinados endereços IP do escopo de qualquer varredura ou Scan;
- 9.2.1.23. A solução deve criptografar todos resultados de varreduras obtidos e informações inseridas tanto em descanso quanto em trânsito;
- 9.2.1.24. A solução deve suportar métodos de autenticação usando bases de autenticação local, e SAML (Security Assertion Markup Language) para uso de SSO (Single Sign-On);

- 9.2.1.25. A solução deve ser capaz de orquestrar Scanners ilimitados dentro da infraestrutura;
- 9.2.1.26. A solução não deve impor nenhum limite de quantidade de Scanners implementados dentro da infraestrutura;
- 9.2.1.27. A solução deverá possuir sistema de alertas para informar a disponibilidade de resultados dos escaneamentos através de Email;
- 9.2.1.28. A solução deve oferecer capacidade de configuração dinâmica de grupos de ativos através de no mínimo as seguintes características:
- 9.2.1.28.1. Sistema Operacional, Endereço IP, DNS, NetBIOS Host, MAC, AWS Instance Type, AWS EC2 Name, Software instalado, Azure VM ID, AWS Region, Google Cloud Instance ID, Azure Resource ID, Ativos avaliados;
- 9.2.2. Dos requisitos e relatórios e painéis gerenciais
- 9.2.2.1. A solução deverá possuir painéis gerenciais (Dashboards) pré-definidos para rápida visualização dos resultados, permitindo ainda a criação de painéis personalizados;
- 9.2.2.2. Os painéis gerenciais deverão ser apresentados em diversos formatos, incluindo gráficos e tabelas, possibilitando a exibição de informações em diferentes níveis de detalhamento;
- 9.2.2.3. Os relatórios devem ser disponibilizados sob demanda no console de gerência da solução;
- 9.2.2.4. Os relatórios devem conter informações da vulnerabilidade, severidade, se existe um Exploit disponível e informações do ativo;
- 9.2.2.5. A solução deve permitir a customização de Dashboards/relatórios;
- 9.2.2.6. A solução deve concentrar todos os relatórios na plataforma central de gerenciamento, não sendo aceitas soluções fragmentadas;
- 9.2.2.7. A solução deve ser capaz de produzir relatórios, pelo menos, nos seguintes formatos: HTML, PDF e CSV;
- 9.2.2.8. A solução deve possibilitar a criação de relatórios baseado nos seguintes alvos: Todos os ativos e Alvos específicos;
- 9.2.2.9. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável);
- 9.2.2.10. A solução deve suportar o envio automático de relatórios para destinatários específicos;
- 9.2.2.11. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;
- 9.2.2.12. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;

9.2.3. Das varreduras

- 9.2.3.1. A solução deve realizar varreduras em uma variedade de sistemas operacionais, incluindo, no mínimo, Windows, Linux e Mac OS, bem como Appliances virtuais;
- 9.2.3.2. A solução deve suportar varredura com e sem agente, de maneira ativa e passiva, distribuídas em diferentes localidades e regiões e gerenciar todos por uma console central;
- 9.2.3.3. A solução deve fornecer agentes instaláveis em sistemas operacionais distintos para monitoramento contínuo de vulnerabilidades;
- 9.2.3.4. Tais agentes devem realizar conexões para o sistema gerenciamento através de protocolo seguro;
- 9.2.3.5. A solução deve ser configurável para permitir a otimização das configurações de varredura;
- 9.2.3.6. A solução deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux;
- 9.2.3.7. A solução deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;
- 9.2.3.8. A solução deve se integrar com solução de gerenciamento de acessos privilegiados para autenticação nos dispositivos, no mínimo, os seguintes:
 - 9.2.3.8.1. CyberArk;
 - 9.2.3.8.2. BeyondTrust;
 - 9.2.3.8.3. Thycotic;
 - 9.2.3.8.4. Centrify;
- 9.2.3.9. A solução deve suportar o agendamento de *Scans* personalizados, incluindo a capacidade de executar varreduras em tempos designados, com frequência pré-determinada;
- 9.2.3.10. A solução deve ser capaz de identificar novos *hosts* no ambiente sem a necessidade de *Scan*;
- 9.2.3.11. A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;
- 9.2.3.12. A solução deve ser capaz de realizar em tempo real a descoberta de vulnerabilidades nas seguintes tecnologias:
 - 9.2.3.12.1. Cloud Services;

- 9.2.3.12.2. Data Leakage;
 - 9.2.3.12.3. Database;
 - 9.2.3.12.4. IoT;
 - 9.2.3.12.5. Mobile Devices;
 - 9.2.3.12.6. Operating System;
 - 9.2.3.12.7. Peer-To-Peer;
 - 9.2.3.12.8. Web Servers;
 - 9.2.3.12.9. Web Clients.
- 9.2.3.13. A solução deve ser capaz de identificar a comunicação de malwares na rede de forma passiva;
- 9.2.3.14. A solução deve, em tempo real, detectar Logins e Downloads de arquivos em um compartilhamento de rede;
- 9.2.4. Da análise e priorização de vulnerabilidades
- 9.2.4.1. A solução deve ser capaz de exibir ambos severidade e pontuação, com base em CVSS (Common Vulnerability Scoring System) e inteligência de ameaças;
 - 9.2.4.2. A solução deve utilizar sistema de pontuação e priorização das vulnerabilidades que utilize no mínimo:
 - 9.2.4.2.1. CVSS Impact Score;
 - 9.2.4.2.2. Idade da Vulnerabilidade;
 - 9.2.4.2.3. Maturidade de códigos de exploração da vulnerabilidade encontrada;
 - 9.2.4.2.4. Frequência de uso da vulnerabilidade em ataques e campanhas atuais;
 - 9.2.4.2.5. Disponibilidade do código de exploração da vulnerabilidade;
 - 9.2.4.2.6. Presença de módulos de exploração de vulnerabilidade em Frameworks automatizados de exploração de vulnerabilidades como CANVAS, Metasploit e Core Impact;
 - 9.2.4.2.7. Popularidade da vulnerabilidade em fóruns e comunicações na *Darkweb*;
 - 9.2.4.2.8. O mecanismo de priorização deve ser sujeito a modificações e atualizações diárias com base em inteligência de ameaças e observação de tendências na *Internet*;
- 9.2.5. Da Análise de Risco do Ambiente

- 9.2.5.1. A solução deve gerar um Score que combine dados de vulnerabilidades com a criticidade dos ativos do ambiente computacional;
- 9.2.5.2. O Score deve ser gerado automaticamente por meio de algoritmos de inteligência artificial (Machine Learning) e deve calcular a probabilidade de exploração de uma determinada vulnerabilidade;
- 9.2.5.3. Deve ser capaz de calcular a criticidade dos ativos da organização;
- 9.2.5.4. A solução deve ser capaz de realizar um Benchmark no ambiente da CONTRATANTE comparando sua maturidade com outras organizações do mesmo setor;
- 9.2.5.5. A solução deve prover visão sobre quais ações de remediação reduzem o maior nível de risco do ambiente;
- 9.2.5.6. A solução deve também permitir a visualização de ações de remediação agregadas para visão consolidada de redução de risco;
- 9.2.5.7. Deve permitir modificar a qualquer momento o tipo de indústria para comparação. Ex: Mudar de Setor Público para Mercado Financeiro;
- 9.2.5.8. Deve fornecer uma lista com as principais recomendações para o ambiente com foco na redução da exposição cibernética da organização;
- 9.2.5.9. A solução deve gerar uma pontuação para cada um dos ativos onde é levado em conta as vulnerabilidades presentes naquele ativo assim como a classificação do ativo na rede (peso do ativo);
- 9.2.5.10. A solução deve gerar uma pontuação global referente a exposição cibernética da organização baseado nas pontuações de cada um dos ativos;
- 9.2.5.11. A solução deve oferecer uma capacidade de comparação (Benchmarking) da pontuação referente a exposição cibernética com outros Players da mesma indústria assim como outras empresas do mercado;
- 9.2.5.12. A solução deve permitir um acompanhamento histórico do nível de exposição da organização;
- 9.2.5.13. Permitir realizar alterações na classificação dos ativos (atribuição de pesos diferentes) podendo sobrescrever a classificação atribuída automaticamente pela solução;
- 9.2.5.14. A solução deverá apresentar indicadores específicos referentes a remediação, possuindo no mínimo informações referentes ao tempo entre remediação e o tempo o qual a vulnerabilidade foi descoberta no ambiente, tempo entre a remediação e a data de publicação da vulnerabilidade, quantidade média de vulnerabilidades críticas por ativo e a comparação da quantidade de vulnerabilidades corrigidas por criticidade;

9.2.5.15. A solução deve permitir a segregação lógica entre áreas distintas da empresa a fim de obter a pontuação referente exposição cibernética por área;

9.2.6. Da descoberta de Ativos:

9.2.6.1. A solução deve ser capaz de realizar escaneamento de descoberta de rede utilizando os seguintes critérios como alvo: IP, CIRD e Range;

9.2.6.2. A solução deve disponibilizar modelos de escaneamento de descoberta, ajustável, com os seguintes tipos de scan:

9.2.6.2.1. Enumeração de Hosts;

9.2.6.2.2. Identificação de Sistema Operacional (SO);

9.2.6.2.3. Port Scan (Portas comuns);

9.2.6.2.4. Port Scan (Todas as portas);

9.2.6.2.5. Customizado;

9.2.6.3. A solução deve permitir realizar escaneamento de descoberta customizado podendo ser parametrizado de acordo com a necessidade;

9.2.6.4. A parametrização do escaneamento de descoberta deve, no mínimo, conter os seguintes requisitos:

9.2.6.4.1. Descoberta de Host;

9.2.6.4.2. Ping o host remoto;

9.2.6.4.3. Usar descoberta rápida;

9.2.6.4.4. Métodos de ping;

9.2.6.4.4.1. ARP;

9.2.6.4.4.2. TCP;

9.2.6.4.4.3. ICMP;

9.2.6.4.4.4. UDP;

9.2.6.4.5. Escaneamento de descoberta em redes de impressora;

9.2.6.4.6. Escaneamento em redes Novell;

9.2.6.4.7. Tecnologia de Wake-on-LAN;

9.2.6.5. Port Scanning:

9.2.6.5.1. Portas;

- 9.2.6.5.1.1. Considerar portas não escaneadas como fechadas;
- 9.2.6.5.1.2. Range de portas a serem escaneadas;
- 9.2.6.6. Enumerar Portas locais:
 - 9.2.6.6.1. SSH (netstat);
 - 9.2.6.6.2. WMI (netstat);
 - 9.2.6.6.3. SNMP;
- 9.2.7. Da descoberta de serviços
 - 9.2.7.1. Sondar todas as portas para encontrar serviços;
 - 9.2.7.2. Procurar por serviços baseado em SSL/TLS;
 - 9.2.7.3. Enumerar todas as cifras SSL/TLS;
- 9.2.8. A solução deve realizar descoberta de ativo de forma passiva e adicionado automaticamente na console de gerenciamento;
- 9.2.9. A solução deve descobrir passivamente quando um *host* é adicionado na rede;
- 9.2.10. Da avaliação de vulnerabilidade
 - 9.2.10.1. A solução deve ser capaz de realizar testes sem a necessidade de agentes instalados no dispositivo destino para detecção de vulnerabilidades;
 - 9.2.10.2. A solução deve detectar e classificar através de severidades, riscos e vulnerabilidades;
 - 9.2.10.3. A solução deve também fornecer informações detalhadas sobre a natureza da vulnerabilidade, evidências da existência da vulnerabilidade e recomendações para mitigá-los;
 - 9.2.10.4. A solução deve incluir uma saída detalhada das vulnerabilidades descobertas como versões de DLL esperadas e encontradas;
 - 9.2.10.5. A solução deve ser compatível com CVE e fornecer pelo menos 10 anos de cobertura CVE;
 - 9.2.10.6. A solução deve identificar vulnerabilidades específicas para o *Active Directory* com os seguintes padrões de verificação:
 - 9.2.10.6.1. Contas administrativas vulneráveis a *Kerberoasting Attack*;
 - 9.2.10.6.2. Utilização de criptografia vulnerável com autenticação *Kerberos*;

- 9.2.10.6.3. Contas com pré-autenticação do *Kerberos* desabilitada;
- 9.2.10.6.4. Verificação de usuários com a opção de nunca expirar a senha com a opção habilitada;
- 9.2.10.6.5. Verificar validação de fragilidades do tipo “Unconstrained Delegation”;
- 9.2.10.6.6. Verificação de “Pre-Windows 2000 Compatible Access”;
- 9.2.10.6.7. Verificação de validade de chaves mestras “Kerberos KRBtgt”;
- 9.2.10.6.8. Verificação de “SID History Injection”;
- 9.2.10.6.9. Verificação de “Printer Bug Exploit”;
- 9.2.10.6.10. Verificação de “*Primary Group ID*”;
- 9.2.10.6.11. Verificação de usuários com *Passwords* em branco;
- 9.2.10.7. A solução deve suportar o uso de SMB e WMI para verificação de sistemas Microsoft Windows;
- 9.2.10.8. A solução deve ser capaz de iniciar automaticamente serviços de registro remoto em sistemas Windows ao executar uma varredura credenciada;
- 9.2.10.9. A solução deve ser capaz de parar automaticamente o serviço de registro remoto em sistemas Windows novamente assim que a varredura estiver completa;
- 9.2.11. O Scanner deve oferecer suporte a Shell seguro (SSH) com a capacidade de escalar privilégios para varredura de vulnerabilidades e auditorias de configuração em sistemas Unix;
- 9.2.11.1. A solução deve suportar o uso do Netstat (Linux) e WMI (Windows) para uma enumeração rápida e precisa de portas em um sistema quando as credenciais são fornecidas;
- 9.2.11.2. A solução deve possibilitar a verificação remota de portas, além da enumeração local de portas, para ajudar a determinar se algum mecanismo de controle de acesso está sendo utilizado;
- 9.2.11.3. A solução deve fornecer auditoria de Patch (MS Bulletins) para as principais versões de Windows;
- 9.2.11.4. A solução deve fornecer auditoria de Patch para todos os principais sistemas operacionais Unix incluindo Mac OS, Linux, Solaris e IBM AIX;
- 9.2.11.5. A solução deve fornecer varredura para aplicativos comerciais diversos e proprietários, incluindo, mas não limitando-se a: Java, Adobe, Oracle, Apple, Microsoft, Check Point, Palo Alto Networks, Cisco, Fortinet, Fireeye, McAfee, etc;

- 9.2.11.6. A solução deve incluir classificação de severidades de acordo com o padrão Sistema Comum de Pontuação de Vulnerabilidade Versão (CVSS2 e CSVSS 3);
- 9.2.11.7. A solução deve fornecer informações acerca da disponibilidade de códigos de exploração das vulnerabilidades encontradas em Frameworks de exploração para as plataformas mais populares: Core, Metasploit e Canvas;
- 9.2.11.8. A solução deve informar se a vulnerabilidade pode e está sendo ativamente explorada por código malicioso (Malware);
- 9.2.11.9. A solução deve possuir importação de arquivos .YARA;
- 9.2.11.10. Deve ser capaz de identificar e classificar vulnerabilidades de máquinas virtuais em nuvem pública em infraestruturas como serviço nas plataformas AWS, Microsoft Azure e Google Cloud;
- 9.2.12. Da auditoria de Configuração
- 9.2.12.1. A solução deve ser capaz de realizar auditoria de conformidade sem a necessidade de agente instalado no dispositivo de destino;
- 9.2.12.2. A solução deve fornecer *Benchmarks* de auditoria de segurança e configuração para conformidade regulatória e outros padrões de práticas recomendadas pela área ou fabricantes;
- 9.2.12.3. A solução deve realizar verificações de auditoria contendo as de segurança, com indicação de sucesso ou falha, baseado nos principais *Frameworks* reconhecidos pela indústria, pelo menos os seguintes:
- 9.2.12.3.1. *Center for Internet Security Benchmarks* (CIS);
 - 9.2.12.3.2. *Defense Information Systems Agency* (DISA) STIGs;
 - 9.2.12.3.3. *Health Insurance Portability and Accountability Act* (HIPAA);
 - 9.2.12.3.4. *Payment Card Industry Data Security Standards* (PCI DSS);
- 9.2.12.4. A solução deve fornecer auditoria de programas antivírus para determinação de presença e *Status* de inicialização para no mínimo os seguintes produtos: TrendMicro Office Scan, McAfee VirusScan, Microsoft Endpoint Protection e Kaspersky;
- 9.2.12.5. A solução deve fornecer auditorias de configuração com base *Benchmarks* em CIS (*Center for Internet Security*) L1 e L2, para ambos os sistemas operacionais Microsoft Windows e Linux;
- 9.2.12.6. A solução deve permitir auditoria de conformidade em servidores Windows, Linux, Bancos de Dados SQL Server, a fim de determinar se estão configurados de acordo com os principais Framework de segurança como, por exemplo, CIS e DISA;

9.2.12.7. A solução deve oferecer validação e suporte a SCAP (*Security Content Automation Protocol*);

9.2.13. Análise dinâmica de vulnerabilidades para aplicações Web

9.2.13.1. A solução deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web como parte dos ativos a serem inspecionados;

9.2.13.2. A solução deve ser capaz de executar varreduras em sistemas web através de seus endereços IP ou FQDN (DNS);

9.2.13.3. A solução deve avaliar no mínimo os padrões de segurança OWASP Top 10 e PCI (*Payment Card Industry Data Security Standard*);

9.2.13.4. A solução deve suportar as diretivas PCI ASV 5.5 para definição de escopo de análise da aplicação;

9.2.13.5. A solução deve suportar as diretivas PCI ASV 6.1 para definição de balanceadores de carga das aplicações bem como suas configurações para inclusão no relatório de resultados;

9.2.13.6. A solução deve possuir *Templates* prontos de varreduras entre simples e extensos;

9.2.13.7. Para varreduras extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos:

9.2.13.7.1. *Cookies, Headers, Formulários e Links*;

9.2.13.7.2. Nomes e valores de parâmetros da aplicação;

9.2.13.7.3. Elementos JSON e XML;

9.2.13.7.4. Elementos DOM;

9.2.13.8. A solução deve permitir somente a execução da função *Crawler*, que consiste na navegação para descoberta das URLs existentes na aplicação;

9.2.13.9. A solução deve ser capaz de utilizar *Scripts* customizados de *Crawl* com parâmetros definidos pelo usuário;

9.2.13.10. A solução deve excluir determinadas URLs da varredura através de expressões regulares;

9.2.13.11. A solução deve excluir determinados tipos de arquivos através de suas extensões;

9.2.13.12. A solução deve instituir no mínimo os seguintes limites:

- 9.2.13.12.1. Número máximo de URLs para *Crawl* e navegação;
- 9.2.13.12.2. Número máximo de diretórios para varreduras;
- 9.2.13.12.3. Número máximo de elementos DOM;
- 9.2.13.12.4. Tamanho máximo de respostas;
- 9.2.13.12.5. Limite de requisições de redirecionamentos;
- 9.2.13.12.6. Tempo máximo para a varredura;
- 9.2.13.12.7. Número máximo de conexões HTTP ao servidor hospedando a aplicação Web;
- 9.2.13.12.8. Número máximo de requisições HTTP por segundo.

- 9.2.13.13. A solução deve detectar congestionamento de rede e limitar os seguintes aspectos da varredura:
 - 9.2.13.13.1. Limite em segundos para *Timeout* de requisições de rede;
 - 9.2.13.13.2. Número máximo de *Timeouts* antes que a varredura seja abortada;

- 9.2.13.14. A solução deve agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;
- 9.2.13.15. A solução deve enviar notificações através de no mínimo *E-mail* e SMS;
- 9.2.13.16. A solução deve possuir a flexibilidade de selecionar quais testes serão realizados de forma granular, através da seleção de testes, *Plug-ins* ou ataques;
- 9.2.13.17. A solução deve avaliar sistemas web utilizando protocolos HTTP e HTTPS;
- 9.2.13.18. A solução deve possibilitar a definição de atributos no cabeçalho (*HEADER*) da requisição HTTP de forma personalizado a ser enviada durante os testes;
- 9.2.13.19. A solução deve ser compatível com avaliação de *Web Services* REST e SOAP;
- 9.2.13.20. Deverá suportar no mínimo os seguintes esquemas de autenticação:
 - 9.2.13.20.1. Autenticação básica (*Digest*);
 - 9.2.13.20.2. NTLM;
 - 9.2.13.20.3. *Form de Login*;
 - 9.2.13.20.4. Autenticação de *Cookies*;
 - 9.2.13.20.5. Autenticação através de *Selenium*;
 - 9.2.13.20.6. Autenticação através de *Bearer*;

- 9.2.13.21. A solução deve importar *Scripts* de autenticação *Selenium* previamente configurados pelo usuário;
- 9.2.13.22. A solução deve customizar parâmetros *Selenium* como *Delay* de exibição da página, *Delay* de execução de comandos e *Delay* de comandos para recepção de novos comandos;
- 9.2.13.23. A solução deve exibir os resultados das varreduras em tendência temporal para acompanhamento de correções e introdução de novas vulnerabilidades;
- 9.2.13.24. A solução deve exibir os resultados agregados de acordo com as categorias do OWASP Top 10 (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project);
- 9.2.13.25. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;
- 9.2.13.26. Para cada vulnerabilidade encontrada, deve ser exibido evidências da mesma em seus detalhes;
- 9.2.13.27. Para vulnerabilidades de injeção de código (SQL, XSS, XSRF etc.), deve evidenciar nos detalhes do evento encontrado:
- 9.2.13.27.1. *Payload* injetado;
 - 9.2.13.27.2. Evidência em forma de resposta da aplicação;
 - 9.2.13.27.3. Detalhes da requisição HTTP;
 - 9.2.13.27.4. Detalhes da resposta HTTP;
- 9.2.13.28. Os detalhes das vulnerabilidades devem conter descrição da falha e referências didáticas para a revisão dos analistas;
- 9.2.13.29. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação das mesmas;
- 9.2.13.30. A solução deve possuir suporte a varreduras de componentes para no mínimo:
- 9.2.13.30.1. Wordpress, Blog Designer Plugin for Wordpress, Event Calendar Plugin for Wordpress, Convert Plus Plugin for Wordpress, AngularJS, Apache, Apache Tomcat, Apache Tomcat JK connecto, Apache Spark e Apache Struts, Atlassian Confluence, Atlassian Crowd e Atlassian Jira, Backbone.js, ASP.NET, Bootstrap, Drupal, Joomla!, jQuery, Lighttpd, Magento, Modernizr, Nginx, PHP, AJAX, Sitefinity, Telerik, ThinkPHP, Webmin e YUI;
- 9.2.14. Solução de análise de infraestrutura sobre código em ambiente de Imagens em Contêiner, DevOps e GitOps.

- 9.2.14.1. A solução deve detectar e configurações incorretas da infraestrutura de nuvem em fases de design, construção e tempo de execução do seu ciclo de vida de desenvolvimento de software;
- 9.2.14.2. A solução deve prevenir problemas de segurança identifique e remova falhas na nuvem durante desenvolvimento antes de chegarem à produção;
- 9.2.14.3. A solução deve ser possível avaliar modelos de infraestrutura como código (IaC), com integrações nativas em:
- 9.2.14.3.1.1. Terraform;
 - 9.2.14.3.1.2. AWS CloudFormation;
 - 9.2.14.3.1.3. Azure Resource Manager;
 - 9.2.14.3.1.4. Kubernetes;
- 9.2.14.4. A solução deve prevenir o desvio de postura na nuvem identifique discrepâncias entre o IaC e sua nuvem em execução ambiente;
- 9.2.14.5. A solução deve fornecer sugestões de correção automaticamente por meio de pull ou mesclagem;
- 9.2.14.6. A solução deve contextualizar riscos compreender as vulnerabilidades de aplicativos no contexto de suas configurações de infraestrutura para obter uma imagem real do risco que eles presente;
- 9.2.14.7. A solução deve prover integração no mínimo com as seguintes plataformas abaixo:
- 9.2.14.7.1.1. Jira;
 - 9.2.14.7.1.2. Slack;
 - 9.2.14.7.1.3. AWS SNS;
 - 9.2.14.7.1.4. Jenkins;
 - 9.2.14.7.1.5. Terraform Cloud;
 - 9.2.14.7.1.6. CircleCI;
 - 9.2.14.7.1.7. Splunk;
 - 9.2.14.7.1.8. AWS CloudTrail;
- 9.2.14.8. A solução deve possuir integração com no mínimo os seguintes Repositórios:
- 9.2.14.8.1.1. Bitbucket;
 - 9.2.14.8.1.2. GitHub;

- 9.2.14.8.1.3. GitLab;
- 9.2.14.8.1.4. Azure DevOps;
- 9.2.14.9. A solução deve possuir funcionalidade de monitoramento dos repositórios sempre que houver alteração de código uma verificação automática via IaC deve apresentar a diferença;
- 9.2.14.10. A solução deve possuir políticas de análise em ambiente de nuvem para no mínimo as seguintes plataformas:
 - 9.2.14.10.1.1. AWS;
 - 9.2.14.10.1.2. Azure;
 - 9.2.14.10.1.3. GCP;
 - 9.2.14.10.1.4. Kubernetes;
- 9.2.15. A solução deve possuir análise por benchmarks e compliance para os seguintes padrões em formato de Dashboard:
 - 9.2.15.1. CIS;
 - 9.2.15.2. NIST;
 - 9.2.15.3. ISO-27001;
 - 9.2.15.4. HIPAA;
 - 9.2.15.5. PCI-DSS;
 - 9.2.15.6. CCM;
 - 9.2.15.7. GDPR;
 - 9.2.15.8. A solução deve analisar, testar e reportar falhas de segurança em aplicações em Containers Docker como parte dos ativos a serem inspecionados;
 - 9.2.15.9. A solução deve ser capaz de analisar imagens preparadas pelos desenvolvedores na esteira DevOps em busca de imagens com vulnerabilidades identificadas e malware residente no sistema de arquivos;
 - 9.2.15.10. A solução deve integrar a esteira DevOps através de API, invocando o envio da imagem para análise em repositório próprio da solução ou utilizando scanner implementado em infraestrutura proprietária do órgão com a finalidade de evitar o envio de imagens e propriedade intelectual da contratante;
 - 9.2.15.11. A documentação de API da solução deverá ter acesso público através de website ou documentação do próprio fabricante;
 - 9.2.15.12. A console de administração deverá possuir controle de acesso no mínimo permitindo

usuários com capacidade de somente visualizar as informações, e usuários com capacidade para efetuar análise das imagens;

- 9.2.15.13. A solução deve inventariar o sistema operacional de cada imagem analisada e suas vulnerabilidades encontradas;
- 9.2.15.14. A solução deve identificar containers que não foram analisados antes de sua implementação em produção;
- 9.2.15.15. A solução deve analisar as camadas (layers) de um container;
- 9.2.15.16. A solução deve identificar containers que tiveram mudanças de arquivos entre a análise e a sua implementação em produção;
- 9.2.15.17. A solução deve informar os CVEs para cada vulnerabilidade encontrada nos pacotes e bibliotecas residentes na imagem;
- 9.2.15.18. A solução deve ter a capacidade de testar automaticamente todas as imagens armazenadas, ou previamente testadas, sempre que uma nova vulnerabilidade for publicada e atualizada no banco de dados de vulnerabilidade da solução, sem qualquer tipo intervenção manual;
- 9.2.15.19. A solução deve inventariar os pacotes e bibliotecas e suas respectivas versões e listar as mesmas dentro do relatório de resultados de análise de cada imagem;
- 9.2.15.20. A solução deve possuir conectores e permitir importação de imagens dos seguintes repositórios:
 - 9.2.15.20.1.1. - Docker;
 - 9.2.15.20.1.2. - Docker EE;
 - 9.2.15.20.1.3. - AWS ECR;
 - 9.2.15.20.1.4. - JFrog Artifactory;
- 9.2.15.21. A solução deve possuir integração com Microsoft Azure Container, Vmware Harbor e Sonatype Nexus para importar e analisar imagens;
- 9.2.15.22. A solução deve fornecer scanner em formato Docker para implementação local e análise de imagens sem a necessidade de envio destas para repositório remoto, fora do ambiente da contratante;
- 9.2.15.23. A solução ser capaz de configurar políticas usando como condições: CVSS Score, CVEs específicos e Malware identificado;
- 9.2.15.24. A solução deve permitir a criação de políticas específicas por repositório;
- 9.2.15.25. A solução deve prover integração com as seguintes plataformas de integração contínua:

Bamboo, CircleCI, Codeship, Distelli, Drone.io, Jenkins, Shippable, Solano Labs, Travis CI, Wrecker e Kubernetes;

9.2.16. Da Análise em ambiente Microsoft *Active Directory*

- 9.2.16.1. A solução deve identificar fraquezas ocultas em configurações dedicadas ao *Active Directory*;
- 9.2.16.2. A solução deve possuir ações preventivas de *Hardening* para o *Active Directory*;
- 9.2.16.3. A solução deve identificar ataque específicos para a estrutura do *Active Directory*;
- 9.2.16.4. A solução deve possuir funcionalidade para analisar em detalhes cada configuração incorreta que acarreta riscos de segurança – com uma linguagem simples, contextualizando tal risco para os times envolvidos;
- 9.2.16.5. A solução deve possuir recomendações de correção para cada configuração incorreta no *Active Directory*;
- 9.2.16.6. A solução deve avaliar relações de confiança perigosas entre florestas e domínios;
- 9.2.16.7. A solução deve capturar as mudanças que ocorrem no AD e demonstrar na console de administração;
- 9.2.16.8. A solução deve possuir *Dashboard* com os principais ataques e vulnerabilidades por domínio;
- 9.2.16.9. A solução deve permitir a correlação de mudanças no *Active Directory* e desvios de segurança;
- 9.2.16.10. A solução deve analisar em detalhes um ataque explorando as descrições através do *Framework* MITRE ATT&CK;
- 9.2.16.11. A solução deve prover interface web para gerenciamento de todas as funcionalidades;
- 9.2.16.12. A solução deve possuir capacidade nativa de criação de *Dashboards* customizados;
- 9.2.16.13. A solução deve suportar um modelo de controle de acesso baseado em funções (RBAC) flexível;
- 9.2.16.14. A solução deve realizar alterações no *Active Directory*, seus objetos e atributos;
- 9.2.16.15. A solução deve armazenar ou sincronizar nenhuma credencial de objetos do *Active Directory*;
- 9.2.16.16. A solução deve suportar ambientes com múltiplas florestas e domínios;

- 9.2.16.17. A solução deve suportar monitoramento contínuo de ambientes com *Active Directory* com o nível funcional de floresta e domínio a partir do 2003;
- 9.2.16.18. A solução deve suportar e reter os eventos coletados por no mínimo um ano;
- 9.2.16.19. A solução deve descobrir e mapear a superfície de ataque do *Active Directory* e seus domínios monitorados com os seguintes padrões:
- 9.2.16.19.1.1. Não depender de agentes ou sensores para coleta de informações do AD;
 - 9.2.16.19.1.2. A solução deve seguir as boas práticas de *menor privilégio*, a conta de serviço utilizada para conexão com o *Active Directory*, sendo o menor nível de acesso esperado para a conta de serviço como parte do grupo *Domain User*;
 - 9.2.16.19.1.3. Interface web que consolida e apresenta de maneira unificada os domínios monitorados e as possíveis relações de confiança estabelecidas entre eles;
- 9.2.16.20. A solução deve analisar continuamente a postura de segurança do AD, minimamente avaliando:
- 9.2.16.20.1. Validação de GPOs desvinculadas, desabilitadas ou órfãs;
 - 9.2.16.20.2. Validação de contas desativadas em grupos privilegiados;
 - 9.2.16.20.3. Domínio usando uma configuração perigosa de compatibilidade com versões anteriores por meio de alterações no atributo *dSHuristics*;
 - 9.2.16.20.4. Validação de atributos relacionados a roaming de credenciais vulneráveis (*ms-PKI-DPAPI MasterKeys*) gerenciados por um usuário sem privilégios;
 - 9.2.16.20.5. Validação de domínio sem GPOs de proteção de computador, desativando protocolos vulneráveis antigos, como *NTLMv1*;
 - 9.2.16.20.6. Validação de contas com senhas que nunca expiram;
 - 9.2.16.20.7. Validação de senhas reversíveis em GPOs;
 - 9.2.16.20.8. Validação de uso de senhas reversíveis em contas de usuário;
 - 9.2.16.20.9. Validação de utilização de protocolo criptográfico fraco (Ex. DES) em contas de usuário;
 - 9.2.16.20.10. Validação de uso do LAPS (Solução de senha de administrador local) para gerenciar senhas de contas locais com privilégios;
 - 9.2.16.20.11. Validação se o domínio possui um nível funcional desatualizado;
 - 9.2.16.20.12. Validação de contas de usuário utilizando senha antiga;

- 9.2.16.20.13. Validação se o atributo *AdminCount* está definido em usuários padrão;
- 9.2.16.20.14. Validação do uso recente da conta de administrador padrão;
- 9.2.16.20.15. Validação de usuários com permissão para ingressar computadores no domínio;
- 9.2.16.20.16. Validação de contas dormentes;
- 9.2.16.20.17. Validação de computadores executando um sistema operacional obsoleto;
- 9.2.16.20.18. Validação de restrições de *Logon* para usuários privilegiados em ambiente com múltiplos *Tiers* (1, 2 e 3) de segregação de ativos;
- 9.2.16.20.19. Validação de direitos perigosos configurados no *Schema* do AD;
- 9.2.16.20.20. Validação de relação de confiança perigosa com outras *Florestas* e *Domínios*;
- 9.2.16.20.21. Validação de contas que possuem um atributo perigoso de histórico SID (*SID History*);
- 9.2.16.20.22. Validação de contas utilizando controle de acesso compatível com versões anteriores ao Windows 2000;
- 9.2.16.20.23. Validação da última alteração de senha do KDC;
- 9.2.16.20.24. Validação da última alteração da senha da conta SSO do *Azure AD*;
- 9.2.16.20.25. Validação de contas que podem ter senha em branco/vazia;
- 9.2.16.20.26. Validação de utilização do grupo nativo *Protected Users*;
- 9.2.16.20.27. Validação de privilégios sensíveis (Ex. *Debug a program*, *Replace a process level token*, etc.) perigosos atribuídos aos usuários;
- 9.2.16.20.28. Validação de possível senha em *Clear-Text*;
- 9.2.16.20.29. Validação de sanidade das GPOs e componentes CSEs (*Client-Side Extension*);
- 9.2.16.20.30. Validação de uso de algoritmos de criptografia fracos na PKI do *Active Directory*;
- 9.2.16.20.31. Validação de contas de serviço com SPN (*Service Principal Name*) que fazem parte de grupos privilegiados;
- 9.2.16.20.32. Validação de contas anormais nos grupos administrativos padrão do AD;
- 9.2.16.20.33. Validação de consistência no *container adminSDHolder*;

- 9.2.16.20.34. Validação de delegação *Kerberos* perigosa;
- 9.2.16.20.35. Validação em permissões de objetos raiz que permitem ataques do tipo *DCSync*;
- 9.2.16.20.36. Validação de políticas de senha fracas aplicadas aos usuários;
- 9.2.16.20.37. Validação das permissões relacionadas às contas do *Azure AD Connect*;
- 9.2.16.20.38. Validação do ID do grupo primário do usuário (*Primary Group ID*);
- 9.2.16.20.39. Validação de permissões em GPOs sensíveis associadas aos *Containers Configuration*, *Sites*, *Root Partition* e *OUs* sensíveis como *Domain Controllers*;
- 9.2.16.20.40. Controladores de domínio gerenciados por usuários ilegítimos;
- 9.2.16.20.41. Validação de certificado mapeado através de atributo *altSecurityIdentities* em contas privilegiadas;
- 9.2.16.20.42. Validação de uso de protocolo *Netlogon* inseguro (*ZeroLogon/CVE-2020-1472*);
- 9.2.16.21. A solução deve identificar vulnerabilidades e configurações incorretas do AD à medida que são introduzidas sendo:
- 9.2.16.21.1. Identificar todas as vulnerabilidades e configurações incorretas no AD;
 - 9.2.16.21.2. Monitorar relações de confiança perigosas em toda a estrutura AD;
 - 9.2.16.21.3. Apresentar ameaças e alterações sem a necessidade de *Scans* estáticos e programados no *Active Directory* e sua infraestrutura;
 - 9.2.16.21.4. Apresentar as ameaças e alterações em tempo real ou em menos de cinco minutos;
- 9.2.16.22. Detecção e resposta a ataques:
- 9.2.16.22.1. Monitorar continuamente os indicadores de possíveis ataque como *DCSync*, *DCShadow*, *Password Spraying*, *Password Guessing/Brute Force*, *Lsaas Injecton* nos controladores de domínio, *Golden Ticket*, *NTLM Relay*, entre outros;
 - 9.2.16.22.2. Detecção de ataques ao AD em tempo real ou em menos de um minuto;
 - 9.2.16.22.3. Análise detalhada do ataque, apresentando ativo de origem, vetor de ataque, controlador de domínio afetado, técnica aplicada;
 - 9.2.16.22.4. Apresentação de ataques em uma linha do tempo;
 - 9.2.16.22.5. Investigar ameaças, reproduzir ataques e procurar por *Backdoors*;

- 9.2.16.22.6. Permitir busca ágil de eventos específicos na base da solução através de queries customizadas;
- 9.2.16.23. A solução deve ser capaz de enviar alertas por e-mail;
- 9.2.16.24. A solução nativamente deve ser capaz de se integrar com SIEM através de protocolo SYSLOG;
- 9.2.16.25. A solução deve ser capaz de filtrar e enriquecer os eventos que serão enviados para o SIEM;
- 9.2.16.26. A solução deve produzir regras YARA na detecção de ataques (Ex. DCSync, Golden Ticket) identificados pela ferramenta;
- 9.2.16.27. A solução deve possuir conjunto de APIs REST, todas as chamadas disponíveis devem estar contidas na documentação;
- 9.2.16.28. A solução deve permitir a criação de listas de exclusões, suportando minimamente Exclusão por domínios do AD monitorados e por itens analisados;
- 9.2.16.29. A solução deve ser licenciada pelo número de usuários habilitados.

9.3. PROCESSO DE EXECUÇÃO DO SERVIÇO PARA GESTÃO DE VULNERABILIDADES

- 9.3.1. A fim de balizar todo o processo de gestão de vulnerabilidade da CONTRATANTE, e influenciado pelos principais *Frameworks* de boas práticas de serviços de segurança da informação, foi arquitetado o processo que será descrito nos parágrafos que seguem, o qual obrigatoriamente a CONTRATADA deve seguir *ipsis litteris*.
- 9.3.2. A CONTRATANTE deverá apresentar uma lista de ativos e recursos que deverão fazer parte do processo de gestão de vulnerabilidade. Tal lista poderá ser revisada e atualizada durante todo o período de vigência de contrato e deverá conter as seguintes informações mínimas, a saber:
 - a) Nome do ativo e/ou serviço;
 - b) Grupo de serviço;
 - c) IP;
 - d) Janela de análise (Horário permitido para análise);
 - e) Prioridade.
- 9.3.3. A CONTRATADA deverá realizar de forma continuada uma avaliação prévia no ambiente computacional da CONTRATANTE a fim de consultivamente sugerir e complementar a lista de ativos e recursos que deverão fazer parte do processo de gestão de vulnerabilidade.
- 9.3.4. De acordo com as variáveis e critérios estabelecidos no catálogo de serviço e na lista de ativos e recursos da CONTRATANTE, a CONTRATADA deverá realizar checagens (*Scans*) e

varreduras, buscando encontrar vulnerabilidades de segurança no ambiente da CONTRATANTE, utilizando as ferramentas e soluções definidas no presente termo de referência.

- 9.3.5. Após o término das rotinas de checagens (*Scans*) e varreduras no ambiente, deverá a CONTRATADA realizar uma análise de falso positivo das vulnerabilidades descobertas, isso quer dizer, que devem ser informadas à CONTRATANTE apenas vulnerabilidades que existam de fato em seu ambiente.
- 9.3.6. Após análise de falso positivo, a CONTRATADA deverá informar ao CONTRATANTE as vulnerabilidades encontradas, obedecendo os critérios e requisitos estabelecidos no presente termo de referência.
- 9.3.7. Uma vez autorizada a mudança para correção de uma determinada vulnerabilidade, caberá a CONTRATADA sugerir as correções de vulnerabilidades encontradas no ambiente listado no tópico AMBIENTE TECNOLÓGICO DA CONTRATANTE (Hardware e Software), obrigatoriamente obedecendo as definições proposta pelo comitê de mudança da CONTRATANTE.
- 9.3.8. Para as vulnerabilidades encontradas no ambiente que ainda não tiverem soluções conhecidas, caberá à CONTRATADA apresentar medidas de contorno, que para aplicá-las ao ambiente, deverá obedecer ao ciclo de mudança estabelecido nos parágrafos anteriores.
- 9.3.9. Como último passo, a CONTRATADA deverá atualizar todos os controles e indicadores estabelecidos no presente termo de referência.
- 9.3.10. O processo descrito é o mínimo esperado a ser seguido e executado pela CONTRATADA. Todavia, como o objeto do presente termo de referência se trata de um serviço continuado, logo, se espera da CONTRATADA a apresentação de melhoria contínua deste, o qual pode ser alterado desde que aprovado pela CONTRATANTE.
- 9.3.11. O ciclo de vida do processo de gestão de vulnerabilidade deve ser executado de forma recorrente. A recorrência é definida em execuções de *Scans* quinzenais e apresentação dos resultados de forma mensal.

9.4. GRUPO TÉCNICO PARA EXECUÇÃO DO SERVIÇO

- 9.4.1. Através do seu Centro de Operações de Segurança definidos e especificados neste certame, a CONTRATADA deverá manter uma torre de operação denominada GRUPO DE ATAQUE CIBERNÉTICO CONTROLADO (Red Team), com objetivo e foco de trabalhar no processo de gestão de vulnerabilidade.
- 9.4.2. Estes profissionais deverão ser exclusivos para trabalhar no GRUPO DE ATAQUE CIBERNÉTICO (Red Team), não podendo os profissionais pertencentes a este grupo serem compartilhados e/ou atuarem com os demais serviços descritos no objeto do presente termo de referência.

- 9.4.3. Todos os profissionais que integram o grupo de ataque cibernético controlado devem obrigatoriamente compor o quadro permanente de colaboradores da CONTRATADA em regime de trabalho CLT (Consolidação das Leis do Trabalho) ou contrato de prestação de serviços firmados diretamente entre esses profissionais e a CONTRATADA, não havendo a possibilidade de terceirização ou subcontratação de tal serviço.
- 9.4.4. Deverá ser de responsabilidade da CONTRATADA dimensionar o número adequado de profissionais para entrega de tal serviço sem que haja impacto no acordo de nível de serviço estabelecido no item Gestão de Vulnerabilidade do presente termo de referência.
- 9.4.5. A fim de garantir que os profissionais envolvidos tenham conhecimento e habilidade para executar o processo de gestão de vulnerabilidades no ambiente da CONTRATANTE, a CONTRATADA obrigatoriamente deverá compor o GRUPO DE ATAQUE CIBERNÉTICO CONTROLADO (*Red Team*) com ao menos 1 (um) perfil de cada que segue descrito abaixo:

Certificações	Descrição
- Linux LPIC 1, Linux LPIC 2 ou Linux LPIC 3 - CompTIA Security+ ou Certified Ethical Hacker	Diploma, devidamente registrado de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.

Tabela 4 - Certificações Grupo de Ataque Cibernético Controlado

- 9.4.6. Não existe restrição ou limite para acúmulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos no GRUPO DE ATAQUE CIBERNÉTICO CONTROLADO (*Red Team*), porém conforme já fora mencionado no presente termo de referência, este(s) deve(m) compor único e exclusivamente o time denominado GRUPO DE ATAQUE CIBERNÉTICO CONTROLADO (*Red Team*).
- 9.4.7. No momento da assinatura do contrato será exigido da CONTRATADA as seguintes documentações do(s) profissionais que participarão do GRUPO DE ATAQUE CIBERNÉTICO CONTROLADO (*Red Team*), os quais devem comprovar as exigências e obrigações descritas no presente termo de referência: contrato de prestação de serviços ou carteira de trabalho devidamente assinada pela CONTRATADA e as devidas certificações técnicas para comprovação do conhecimento.

9.5. ENTREGAS A SEREM REALIZADAS

Rua Cláudio Manoel, 639 - Savassi – Belo Horizonte/MG – Cep: 30140-105
 Telefone: (31) 3269-8400 - www.crcmg.org.br

- 9.5.1. Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, a CONTRATANTE definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue de forma *On Line* e em tempo de execução, através do portal de segurança descrito no tópico de condições gerais para prestação do serviço deste termo de referência, a saber:

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Quantitativo de vulnerabilidades	Soma de vulnerabilidades	Vulnerabilidades	Vulnerabilidades	Número total de vulnerabilidades
Quantitativo de vulnerabilidades de severidade 5 por área responsável	Soma de vulnerabilidades de severidade 5 por área responsável	Vulnerabilidades de severidade 5	Vulnerabilidades	Número total de vulnerabilidades de severidade 5 por área responsável
Quantitativo de vulnerabilidades de severidade 4 por área responsável	Soma de vulnerabilidades de severidade 4 por área responsável	Vulnerabilidades de severidade 4	Vulnerabilidades	Número total de vulnerabilidades de severidade 4 por área responsável
Quantitativo de novas vulnerabilidades de severidades 4 e 5 por área responsável	Soma de novas vulnerabilidades de severidades 4 e 5 por área responsável	Vulnerabilidades de severidades 4 e 5	Vulnerabilidades	Número total de novas vulnerabilidades de severidades 4 e 5 por área responsável
Quantitativo de vulnerabilidades corrigidas de severidades 4 e 5 por área responsável	Soma de vulnerabilidades corrigidas de severidades 4 e 5 por área responsável	Vulnerabilidades corrigidas de severidades 4 e 5	Vulnerabilidades	Número total de vulnerabilidades corrigidas de severidades 4 e 5 por área responsável
Quantitativo de vulnerabilidades em Aplicações WEB	Soma de vulnerabilidades em Aplicações WEB	Vulnerabilidades em Aplicações WEB	Vulnerabilidades	Número total de vulnerabilidades em Aplicações WEB
Quantitativo de vulnerabilidades em Aplicações WEB de severidade 5	Soma de vulnerabilidades em Aplicações WEB de severidade 5	Vulnerabilidades em Aplicações WEB de severidade 5	Vulnerabilidades	Número total de vulnerabilidades em Aplicações WEB de severidade 5
Quantitativo de vulnerabilidades em Aplicações WEB de severidade 4	Soma de vulnerabilidades em Aplicações WEB de severidade 4	Vulnerabilidades em Aplicações WEB de severidade 4	Vulnerabilidades	Número total de vulnerabilidades em Aplicações WEB de severidade 4

Quantitativo de novas vulnerabilidades em Aplicações WEB de severidades 4 e 5	Soma de novas vulnerabilidades em Aplicações WEB de severidades 4 e 5	Vulnerabilidades em Aplicações WEB de severidades 4 e 5	Vulnerabilidades	Número total de novas vulnerabilidades em aplicações WEB de severidades 4 e 5
Quantitativo de vulnerabilidades corrigidas em Aplicações WEB de severidades 4 e 5	Soma de vulnerabilidades corrigidas em Aplicações WEB de severidades 4 e 5	Vulnerabilidades corrigidas em Aplicações WEB de severidades 4 e 5	Vulnerabilidades	Número total de vulnerabilidades corrigidas em Aplicações WEB de severidades 4 e 5
Quantitativo de certificados digitais expirados	Soma de certificados digitais expirados	Certificados digitais expirados	Certificados digitais	Número total de certificados digitais expirados
Quantitativo de certificados digitais a expirar em 3 meses	Soma de certificados digitais a expirar em 3 meses	Certificados digitais a expirar em 3 meses	Certificados digitais	Número total de certificados digitais a expirar em 3 meses
TOP 10 – Ativos mais vulneráveis	Soma de vulnerabilidades por ativo	Vulnerabilidades por ativo	Vulnerabilidades	TOP 10 do número de vulnerabilidades por ativo
TOP 10 – Vulnerabilidades mais comuns em ativos	Soma de vulnerabilidades	Vulnerabilidades	Vulnerabilidades	TOP 10 do número de vulnerabilidades
TOP 10 – Áreas responsáveis com maior número de vulnerabilidades	Soma de vulnerabilidades por área responsável	Vulnerabilidades por área responsável	Vulnerabilidades	TOP 10 do número de vulnerabilidades por área responsável
TOP 10 – Áreas responsáveis com maior número de vulnerabilidades de severidade 4 e 5	Soma de vulnerabilidades de severidade 4 e 5 por área responsável	Vulnerabilidades de severidade 4 e 5 por área responsável	Vulnerabilidades	TOP 10 do número de vulnerabilidades de severidade 4 e 5 por área responsável
TOP 10 – Áreas responsáveis com percentual de vulnerabilidades	Percentual de vulnerabilidades de severidade 4 e 5 por área responsável	Vulnerabilidades de severidade 4 e 5 por área responsável	Vulnerabilidades	TOP 10 do percentual de vulnerabilidades de severidade 4 e 5 por área responsável

de severidade 4 e 5				
TOP 10 – Aplicações WEB mais vulneráveis	Soma de vulnerabilidades em Aplicações WEB	Vulnerabilidades em Aplicações WEB	Vulnerabilidades	TOP 10 do número total de vulnerabilidades em Aplicações WEB
TOP 10 – Aplicações WEB mais vulneráveis em comparação com OWASP	Soma de vulnerabilidades em Aplicações WEB em comparação com OWASP	Vulnerabilidades em Aplicações WEB	Vulnerabilidades	TOP 10 do número total de vulnerabilidades em Aplicações WEB em comparação com OWASP

Tabela 5 - Indicadores Estratégicos Gestão de Vulnerabilidade

10. MONITORAMENTO, DETECÇÃO E RESPOSTA A INCIDENTES PARA ENDPOINTS

- 10.1.1. A operação e gerenciamento de proteção avançada de *Endpoint* deverá seguir os preceitos técnicos definidos abaixo com o intuito da CONTRATADA ofertar plataforma de gestão avançada de segurança para *Endpoint*, agregando qualidade e mais proteção ao processo;
- 10.1.2. Cabe à CONTRATADA toda operação, dos níveis mais básicos (Nível 1) até o mais avançado (Nível 3).
- 10.1.3. Deverá ser criado usuário de leitura para equipe da CONTRATANTE, limitado à 4 profissionais de segurança da informação, para acompanhamento das ações na console de gerenciamento.
- 10.1.4. SOBRE A FERRAMENTA A SER UTILIZADA
 - 10.1.4.1. Realizar a pré-execução do agente para verificar o comportamento malicioso e detectar *Malware* desconhecido;
 - 10.1.4.2. O agente deve buscar algum sinal de *Malware* ativo e detectar *Malwares* desconhecidos;
 - 10.1.4.3. O agente deve ter a capacidade de submeter o arquivo desconhecido à nuvem de inteligência do fabricante para detectar a presença de ameaças;
 - 10.1.4.4. O agente deve realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes;
 - 10.1.4.5. A solução deve manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência;
 - 10.1.4.6. Deve realizar a verificação de todos os arquivos acessados em tempo real, mesmo durante o processo de *Boot*;
 - 10.1.4.7. Deve realizar a verificação de todos os arquivos no disco rígido em intervalos programados;

- 10.1.4.8. Deve realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA);
- 10.1.4.9. Deve proteger os navegadores Internet Explorer, Firefox, Chrome, Opera, Safari e Microsoft Edge, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados;
- 10.1.4.10. Deve permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos;
- 10.1.4.11. É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, *Spyware*, *Trojans*, *Worms*, *Adware* e aplicativos potencialmente indesejados (PUAs);
- 10.1.4.12. Suportar equipamentos com arquitetura 32-bit e 64-bit que o cliente deve ter instalado nas estações de trabalho e deve ser compatível com os sistemas operacionais: Mac OS X 10.10, 10.11, 10.12, Microsoft Windows XP SP3, 7, e 10;
- 10.1.4.13. Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção;
- 10.1.4.14. Permitir a utilização de senha de proteção para permitir a reconfiguração local no cliente ou desinstalação dos componentes de proteção;
- 10.1.4.15. Funcionalidade de Firewall e Detecção e Proteção de Intrusão para estação com as funcionalidades:
- 10.1.4.16. Deve possuir atualização periódica de novas assinaturas de ataque;
- 10.1.4.17. Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (*Hash*) do arquivo;
- 10.1.4.18. Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas;
- 10.1.4.19. Possuir um sistema de prevenção de intrusão na estação (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados.
- 10.1.4.20. Deve aplicar uma análise adicional, inspecionando finalmente o comportamento de códigos durante a execução, para detectar comportamento suspeito de aplicações, tais como *Buffer Overflow*.
- 10.1.4.21. Deve possuir técnicas de proteção, que inclui:
- 10.1.4.22. Análise dinâmica de código - técnica para detectar *Malware* criptografado mais complexo;

- 10.1.4.23. Algoritmo correspondente padrão - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificados como um vírus;
 - 10.1.4.24. Possuir capacidade para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;
 - 10.1.4.25. Possuir tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo. jpg.txt) ou a extensão não coincide com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt);
 - 10.1.4.26. Verificação de ameaças web avançadas: bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise comportamental para identificar e parar o código malicioso de *Malware* avançado.
- 10.1.5. Funcionalidades de Antivírus e *Antispyware*
- 10.1.5.1. Proteção em tempo real contra vírus, *Trojans*, *Worms*, *Rootkits*, *Botnets*, *Spyware*, *Adwares* e outros tipos de códigos maliciosos.
 - 10.1.5.2. Proteção *Anti-Malware* nativa da solução ou incorporada automaticamente por meio de *Plug-ins* sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante.
 - 10.1.5.3. As configurações do *Anti-Spyware* deverão ser realizadas através da mesma console do antivírus;
 - 10.1.5.4. Permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou *Malware*, permitir a inclusão de arquivos em listas de exclusão (*Whitelists*) para que não sejam verificados pelo produto;
 - 10.1.5.5. Permitir a varredura das ameaças da maneira manual, agendada e em tempo real na máquina do usuário;
 - 10.1.5.6. Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos, através do antivírus;
 - 10.1.5.7. Capacidade de remoção automática total dos danos causados por *Spyware*, *Adwares* e *Worms*, como limpeza do registro e pontos de carregamento, com opção de finalizar o processo e terminar o serviço da ameaça no momento de detecção;
 - 10.1.5.8. A remoção automática dos danos causados deve ser nativa do próprio antivírus; ou adicionada por plugin, desde que desenvolvido ou distribuído pelo fabricante;
 - 10.1.5.9. Capacidade de bloquear origem de infecção através de compartilhamento de rede com opção de bloqueio da comunicação via rede;

- 10.1.5.10. Permitir o bloqueio da verificação de vírus em recursos mapeados da rede;
- 10.1.5.11. Antivírus de Web (verificação de *Sites* e *Downloads* contra vírus);
- 10.1.6. Controle de Acesso a *Sites* por Categoria
 - 10.1.6.1. Proteger a navegação na *Web*, mesmo aos usuários fora da rede, para todos os principais navegadores (IE, Firefox, Safari, Opera, Chrome e Microsoft Edge), fornecendo controle da *Internet* independentemente do *Browser* utilizado, como parte da solução de proteção a estações de trabalho, incluindo a análise do conteúdo baixado pelo navegador *Web*, de forma independente do navegador usado, ou seja, sem utilizar um *Plugin*, onde não é possível ser ignorada pelos usuários, protegendo os usuários de *Websites* infectados.
 - 10.1.6.2. Funcionalidades específicas para prevenção contra a ação de *Ransomwares*, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos ou a capacidade de fazer *Backup* de arquivos antes de serem criptografados para posteriormente permitir sua restauração.
- 10.1.7. Funcionalidade de detecção Pró-Ativa de reconhecimento de novas ameaças.
 - 10.1.7.1. Funcionalidade de detecção de ameaças via técnicas de *Deep Machine Learning*;
 - 10.1.7.2. Funcionalidade de detecção de ameaças desconhecidas que estão em memória;
 - 10.1.7.3. Capacidade de detecção, e bloqueio pró-ativo de *Keyloggers* e outros *Malwares* não conhecidos (ataques de dia zero) através da análise de comportamento de processos em memória (heurística);
 - 10.1.7.4. Capacidade de detecção e bloqueio de *Trojans* e *Worms*, entre outros *Malwares*, por comportamento dos processos em memória;
 - 10.1.7.5. Capacidade de analisar o comportamento de novos processos ao serem executados, em complemento à varredura agendada.
- 10.1.8. Funcionalidades de proteção contra *Ransomware*
 - 10.1.8.1. Dispor de proteção contra *Ransomware* não baseada exclusivamente na detecção por assinaturas;
 - 10.1.8.2. Dispor de remediação da ação de criptografia maliciosa dos *Ransomwares*;
 - 10.1.8.3. A solução deve prevenir ameaças e interromper que eles sejam executados em dispositivos da rede, detectando e limpando os *Malwares*, além da realização de uma análise detalhada das alterações realizadas.
 - 10.1.8.4. Possuir uma tecnologia *Anti-Exploit* baseada em comportamento, reconhecendo e

bloqueando as mais comuns técnicas de *Malware*, protegendo os *Endpoints* de ameaças desconhecidas e vulnerabilidades *Zero-Day*.

10.1.8.5. Deve ser realizada a detecção e o bloqueio de, pelo menos, as seguintes técnicas de exploit:

- a) DEP (Data Execution Prevention);
- b) Address Space Layout Randomization (ASLR);
- c) Bottom Up ASLR;
- d) Null Page;
- e) Anti-HeapSpraying;
- f) Dynamic Heap Spray;
- g) Import Address Table Filtering (IAF);
- h) VTable Hijacking;
- i) Stack Pivot and Stack Exec;
- j) SEHOP;
- k) Stack-based ROP (Return-Oriented Programming);
- l) Control-Flow Integrity (CFI);
- m) Syscall;
- n) WOW64;
- o) Load Library;
- p) Shellcode;
- q) VBScript God Mode;
- r) Application Lockdown;
- s) Process Protection;
- t) Network Lockdown;
- u) Remote reflective DLL injection;

10.1.8.6. *Local Privilege Escalation* – LPE.

10.1.8.7. A solução deve trabalhar silenciosamente na máquina do usuário e deve detectar a criptografia maliciosa de dados (*Ransomware*), realizando a sua interrupção. No caso de arquivos serem criptografados a solução deve realizar o retorno destes arquivos ao seu estado normal. Deste modo a solução deve fazer a limpeza e remoção completa do *Ransomware* na máquina do usuário.

10.1.8.8. Deve fornecer também uma análise detalhada das modificações realizadas pelo *Ransomware*, realizando a correlação dos dados em tempo real, indicando todas as

modificações feitas em registros, chaves, arquivos alvos, conexões de redes e demais componentes contaminados.

- 10.1.8.9. A console de monitoração e configuração deve ser feita através de uma central única, baseada em *Web* e em nuvem ou *Appliance* físico, que deve conter todas as ferramentas para a monitoração e controle da proteção dos dispositivos para a solução de *Anti-Exploit* e *Anti-Ransomware*.
- 10.1.8.10. A console deve apresentar painel com o resumo detalhado de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional, bem como todas as identificações para o mapeamento instantâneo dos efeitos causados pelo *Ransomware* nas estações de trabalho.
- 10.1.8.11. A solução deve implementar técnicas de EDR (*Endpoint Detection and Response*), possibilitando detecção e investigação nos *Endpoints* com atividades suspeitas;
- 10.1.8.12. Em caso de incidente a solução deve mostrar a trilha da infecção de forma visual, mostrando o início, todas as interações do *Malware* e o ponto final de bloqueio.
- 10.1.8.13. Após a análise da nuvem de inteligência do fabricante a solução deve apresentar um relatório sobre a ameaça contendo no mínimo:
- 10.1.8.14. Detalhes do Processo, como nome, *Hash*, hora e data da detecção e remediação;
- 10.1.8.15. Resultado da análise do arquivo suspeito pela funcionalidade de *Machinne Learning* ou *Deep Learning*;
- 10.1.8.16. Propriedades gerais do arquivo, como nome, versão, tamanho, idioma, informações de certificado;
- 10.1.8.17. A solução de EDR deve ser integrada ao agente de antivírus, instalada como um agente único em estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;
- 10.1.8.18. O gerenciamento da solução de EDR deve ser feito a partir da mesma Console de Gerenciamento da solução antivírus;
- 10.1.8.19. Deve fornecer guias de respostas a incidentes, fornecendo visibilidade sobre o escopo de um ataque, como ele começou, o que foi impactado, e como responder;
- 10.1.8.20. Deve responder ao incidente com opção de isolamento da máquina, bloqueio e limpeza da ameaça;
- 10.1.8.21. Deve realizar buscas de ameaças em todo o ambiente, permitir buscar por *Hash*, nome, endereços IP, domínio ou linha de comando;
- 10.1.8.22. Funcionalidade de Controle de Aplicações e Dispositivos Externos:

- 10.1.8.23. Possuir controle de aplicativos para monitorar e impedir que os usuários executem ou instalem aplicações que podem afetar a produtividade ou o desempenho da rede;
- 10.1.8.24. Atualizar automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicativos específicos ou categorias específicas de aplicações possam ser liberadas ou bloqueadas;
- 10.1.8.25. Verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões. Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web;
- 10.1.8.26. Oferecer proteção para chaves de registro e controle de processos;
- 10.1.8.27. Proibir através de política a inicialização de um processo ou aplicativo com base no nome e no *Hash* do arquivo;
- 10.1.8.28. Detectar um aplicativo controlado quando os usuários o acessarem, com as opções de permitir e alertar ou bloquear e alertar;
- 10.1.8.29. Possuir a opção de customizar uma mensagem a ser mostrada ao usuário em caso de bloqueio de execução do aplicativo;
- 10.1.8.30. Gerenciar o uso de dispositivos de armazenamento USB (ex: pen-drives e HDs USB). Permitir, através de regras, o bloqueio ou liberação da leitura/escrita/execução do conteúdo desses dispositivos;
- 10.1.8.31. Controlar o uso de outros dispositivos periféricos, como comunicação infravermelha e modem externo;
- 10.1.8.32. As funcionalidades do Controle de Aplicações e Dispositivos deverão ser nativas do produto ou incorporadas automaticamente por meio de *Plugins* sem utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante;
- 10.1.8.33. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
- 10.1.8.34. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
- 10.1.8.35. A gestão desses dispositivos deve ser feita diretamente na Console de Gerenciamento, deve permitir definir políticas diferentes por grupos de *Endpoints*;
- 10.1.8.36. Permitir a autorização de um dispositivo com no mínimo as seguintes opções:
 - a) Permitir que todos os dispositivos do mesmo modelo;
 - b) Permitir que um único dispositivo com base em seu número de identificação único;
 - c) Permitir o acesso total;

d) Permitir acesso somente leitura.

10.1.9. Funcionalidades Contra-Ataques Avançados, Detecção e Resposta.

- 10.1.9.1. A solução deve ter capacidade de implementar técnicas avançada contra-ataque, detecção e resposta, possibilitando detecção e investigação nas estações de trabalho com atividades suspeitas;
- 10.1.9.2. Em caso de incidente a solução deve mostrar a trilha da infecção de forma visual, mostrando o início, todas as interações do *Malware* e o ponto final de bloqueio.
- 10.1.9.3. Após a análise da nuvem de inteligência do fabricante a solução deve apresentar um relatório sobre a ameaça contendo no mínimo:
- 10.1.9.4. Detalhes do Processo, como nome, *Hash*, hora e data da detecção e remediação;
- 10.1.9.5. Reputação do arquivo e correlação da detecção do arquivo em outras soluções de antivírus através de bases de conhecimento como o Vírus Total ou do próprio fabricante;
- 10.1.9.6. Resultado da análise do arquivo suspeito pela funcionalidade de *Machinne Learning* ou *Deep Learning*;
- 10.1.9.7. Propriedades gerais do arquivo, como nome, versão, tamanho, idioma, informações de certificado;
- 10.1.9.8. A solução de EDR (*Endpoint Detection and Response*) deve ser integrada ao agente de antivírus, instalada como um agente único em estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;
- 10.1.9.9. O gerenciamento da solução de EDR deve ser feito a partir da mesma console de gerenciamento da solução antivírus;
- 10.1.9.10. Deve fornecer guias de respostas a incidentes, fornecendo visibilidade sobre o escopo de um ataque, como ele começou, o que foi impactado, e como responder;
- 10.1.9.11. Deve responder ao incidente com opção de isolamento da máquina, bloqueio e limpeza da ameaça;
- 10.1.9.12. Deve realizar buscas de ameaças em todo o ambiente, permitir buscar por *Hash*, nome, endereços IP, domínio ou linha de comando;

10.1.10. Funcionalidade de Controle de Aplicações e Dispositivos:

- 10.1.10.1. Oferecer proteção para chaves de registro e controle de processos;
- 10.1.10.2. Proibir, através de política a inicialização de um processo ou aplicativo, com base no

nome e no *Hash* do arquivo;

- 10.1.10.3. Gerenciar o uso de dispositivos de armazenamento USB (ex: pen-drives e HDs USB). Permitir, através de regras, o bloqueio ou liberação da leitura/escrita/execução do conteúdo desses dispositivos;
- 10.1.10.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
- 10.1.10.5. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
- 10.1.10.6. A gestão desses dispositivos deve ser feita diretamente na console de gerenciamento e permitir definir políticas diferentes por grupos de *Endpoints*;
- 10.1.10.7. Permitir a autorização de um dispositivo com no mínimo as seguintes opções:
 - a) Permitir todos os dispositivos do mesmo modelo;
 - b) Permitir um único dispositivo com base em seu número de identificação único;
 - c) Permitir o acesso total;
 - d) Permitir acesso somente leitura.
- 10.1.10.8. Proteger servidores contra *Malwares*, arquivos e tráfego de rede malicioso, controle de periféricos, controle de acesso à web, controle de aplicativos em um único agente instalado nos servidores;
- 10.1.10.9. Realizar a pré-execução do agente para verificar o comportamento malicioso e detectar *Malwares* desconhecidos;
- 10.1.10.10. O agente *Host* deve buscar algum sinal de *Malwares* ativos e detectar *Malwares* desconhecidos;
- 10.1.10.11. O agente deve realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes;
- 10.1.10.12. A solução deve manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência;
- 10.1.10.13. Realizar a verificação de todos os arquivos acessados em tempo real, mesmo durante o processo de *Boot*;
- 10.1.10.14. Realizar a verificação de todos os arquivos no disco rígido em intervalos programados;
- 10.1.10.15. Realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA);
- 10.1.10.16. Proteger os navegadores Internet Explorer, Firefox, Chrome, Opera, Safari e Microsoft

Edge, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados;

- 10.1.10.17. Permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos;
- 10.1.10.18. É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, *Spyware*, *Trojans*, *Worms*, *Adware* e aplicativos potencialmente indesejados (PUAs);
- 10.1.10.19. O cliente para instalação em servidores deve ser compatível com os sistemas operacionais abaixo:
 - a) Windows Server 2022;
 - b) Windows Server 2019;
 - c) Windows Server 2016;
 - d) Windows Server 2012 R2 (64 bit);
 - e) Windows Server 2012 (64 bit);
 - f) Windows Server 2008 R2 (64 bit);
 - g) Ubuntu (versão atual 20.04 ou superior).
- 10.1.10.20. Suportar a inclusão de outros servidores para a função de atualização distribuída e cache, de forma a agilizar o processo de atualização dos demais agentes;
- 10.1.10.21. Possuir integração com as nuvens da Microsoft Azure e Amazon Web Services para identificar as informações dos servidores instanciados nas nuvens;
- 10.1.10.22. Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção;
- 10.1.10.23. Permitir a utilização de senha de proteção para permitir a reconfiguração local no cliente ou desinstalação dos componentes de proteção;
- 10.1.10.24. Funcionalidade de *Firewall* e Detecção e Proteção de Intrusão (IDS/IPS);
- 10.1.10.25. Possuir proteção contra exploração de *Buffer Overflow*;
- 10.1.10.26. Possuir proteção contra ataques de Negação de Serviço (Denial of Service - DoS), Port-Scan, MAC Spoofing e IP Spoofing;
- 10.1.10.27. Possuir atualização periódica de novas assinaturas de ataque;

- 10.1.10.28. Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (*Hash*) do arquivo.
- 10.1.10.29. Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas;
- 10.1.10.30. Possuir um sistema de prevenção de intrusão no *Host* (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados.
- 10.1.10.31. Identificar comportamentos suspeitos de códigos e ataques de dia zero (*Zero Day*), tais como: *Buffer Overflow*, tráfego de códigos maliciosos e atividades suspeitas detectadas por comportamento.
- 10.1.10.32. Possuir técnicas de proteção, que inclui:
- a) Análise dinâmica de código - técnica para detectar *Malware* criptografado mais complexo;
 - b) Algoritmo correspondente padrão - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificado como um vírus;
 - c) Possuir capacidade para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;
 - d) Possuir tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo. jpg.txt) ou a extensão não coincida com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt);
 - e) Verificação de ameaças *Web* avançadas: bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise comportamental para identificar e parar o código malicioso de *Malware* avançados.
- 10.1.11. Funcionalidade de Antivírus e *AntiSpyware*:
- 10.1.11.1. Proteção em tempo real contra vírus, *Trojans*, *Worms*, *Rootkits*, *Botnets*, *Spyware*, *Adwares* e outros tipos de códigos maliciosos.
- 10.1.11.2. Proteção *Anti-Malware* nativa da solução ou incorporada automaticamente por meio de *Plug-Ins* sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante.
- 10.1.11.3. As configurações do *Anti-Spyware* devem ser realizadas através da mesma console do antivírus;
- 10.1.11.4. Permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou *Malware*, permitir a inclusão de arquivos em listas de exclusão (*Whitelists*)

para que não sejam verificados pelo produto;

- 10.1.11.5. Permitir a varredura das ameaças da maneira manual, agendada e em tempo real nos servidores;
- 10.1.11.6. Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do antivírus;
- 10.1.11.7. Capacidade de detectar arquivos através da reputação dos mesmos;
- 10.1.11.8. Capacidade de remoção automática total dos danos causados por *Spyware*, *Adwares* e *Worms*, como limpeza do registro e pontos de carregamento, com opção de finalizar o processo e terminar o serviço da ameaça no momento de detecção;
- 10.1.11.9. A remoção automática dos danos causados deve ser nativa do próprio antivírus; ou adicionada por *Plugin*, desde que desenvolvido ou distribuído pelo fabricante;
- 10.1.11.10. Bloquear origem de infecção através de compartilhamento de rede com opção de bloqueio da comunicação via rede;
- 10.1.11.11. Detectar tráfego de rede para comandar e controlar os servidores;
- 10.1.11.12. Proteger arquivos de documento contra-ataque do tipo *Ransomwares*;
- 10.1.11.13. Proteger contra ataques de *Ransomware* em pastas compartilhadas na rede;
- 10.1.11.14. Permitir o envio de amostras de *Malwares* para a nuvem de inteligência do fabricante;
- 10.1.11.15. Permitir o bloqueio da verificação de vírus em recursos mapeados da rede;
- 10.1.11.16. Antivírus de *Web* (verificação de *Sites* e *Downloads* contra vírus).
- 10.1.12. Gerenciamento e administração centralizada
 - 10.1.12.1. A console de monitoração e configuração deve ser feita através de uma central para o grupo de *Anti-Malware*, baseada em *Web* e em nuvem ou *Appliance*, que deve conter todas as ferramentas para a monitoração e controle da proteção dos dispositivos;
 - 10.1.12.2. A console deve apresentar painel com o resumo dos *Status* de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional;
 - 10.1.12.3. Possuir mecanismo de comunicação via API, Syslog ou RESTFULL API (*Representational State Transfer*), para integração com outras soluções de segurança, disponibilizando acesso a documentação técnica da API do fabricante;
 - 10.1.12.4. A console deve permitir a divisão dos computadores, dentro da estrutura de

gerenciamento em grupos;

- 10.1.12.5. Permitir sincronização com o *Active Directory* (AD) para gestão de usuários e grupos integrados às políticas de proteção.
- 10.1.12.6. Aplicar regras diferenciadas baseado em grupos ou usuários;
- 10.1.12.7. A instalação deve ser feita via cliente específico por *Download* da gerência central ou também via *Email* de configuração. O instalador deve permitir a distribuição do cliente via *Active Directory* (AD) para múltiplas máquinas;
- 10.1.12.8. A console deve permitir criar e editar diferentes políticas para a aplicação das proteções exigidas e aplicadas a nível de usuários ou *Endpoint*, não importando em que equipamentos eles estejam acessando;
- 10.1.12.9. Fornecer atualizações do produto e das definições de vírus e proteção contra intrusos;
- 10.1.12.10. Permitir exclusões de escaneamento para um determinado *Website*, pasta, arquivo ou aplicação, tanto a nível geral quanto específico em uma determinada política.
- 10.1.12.11. A console de gerenciamento deve permitir a definição de grupos de usuários com diferentes níveis de acesso as configurações, políticas e *Logs*;
- 10.1.12.12. Atualização incremental, remota e em tempo-real, da vacina dos antivírus e do mecanismo de verificação (*Engine*) dos clientes;
- 10.1.12.13. Permitir o agendamento da varredura contra vírus, permitir selecionar uma máquina, grupo de máquinas ou domínio, com periodicidade definida pelo administrador;
- 10.1.12.14. Atualização automática das assinaturas de ameaças (*Malwares*) e políticas de prevenção desenvolvidas pelo fabricante em tempo real ou com periodicidade definida pelo administrador;
- 10.1.12.15. Utilizar protocolos seguros padrão HTTPS para comunicação entre console de gerenciamento e clientes gerenciados.
- 10.1.12.16. As mensagens geradas pelo agente devem estar no idioma em português ou permitir a sua edição.
- 10.1.12.17. Recursos do relatório e monitoramento devem ser nativos da própria console central de gerenciamento;
- 10.1.12.18. Exibir informações como nome da máquina, versão do antivírus, sistema operacional, versão da *Engine*, data da vacina, data da última verificação, eventos recentes e *Status*;
- 10.1.12.19. Capacidade de geração de relatórios, estatísticos ou gráficos, tais como:

- 10.1.12.20. Detalhar quais usuários estão ativos, inativos ou desprotegidos, bem como detalhes dos mesmos;
- 10.1.12.21. Detalhamento dos computadores que estão ativos, inativos ou desprotegidos, bem como detalhes das varreduras e dos alertas nos computadores;
- 10.1.12.22. Detalhamento dos periféricos permitidos ou bloqueados, bem como detalhes de onde e quando cada periférico foi usado;
- 10.1.12.23. Detalhamento das principais aplicações bloqueadas e os servidores/usuários que tentaram acessá-las;
- 10.1.12.24. Detalhamento das aplicações permitidas que foram acessadas com maior frequência e os servidores/usuários que as acessam;
- 10.1.12.25. Detalhamento dos servidores/usuários que tentaram acessar aplicações bloqueadas com maior frequência e as aplicações que eles tentaram acessar;
- 10.1.12.26. Detalhamento de todas as atividades disparadas por regras de prevenção de perda de dados.
- 10.1.12.27. Possuir um elemento de comunicação para mensagens e notificações entre estações e a console de gerenciamento utilizando comunicação criptografada;
- 10.1.12.28. Fornecer solução de gerenciamento de arquivos armazenados em nuvem, garantindo que um arquivo que foi feito um *Upload* (exemplo Dropbox, Google Drive, OneDrive), tenha o processo monitorado e gerenciado, bem como realizar automaticamente o escaneamento do arquivo contra *Malwares*, procuradas palavras chaves ou informações confidenciais. Deve ser bloqueado o *Upload* ou removida a informação confidencial antes do envio do arquivo;
- 10.1.12.29. As portas de comunicação deverão ser configuráveis. A comunicação deve permitir QoS para controlar a largura de banda de rede.
- 10.1.12.30. A solução deve permitir a seleção da versão do *Software* de preferência, permitindo assim o teste da atualização sobre um grupo de PCs piloto antes de implantá-lo para toda a rede. Permitir ainda selecionar um grupo de computadores para aplicar a atualização para controlar a largura de banda de rede. A atualização da versão deve ser transparente para os usuários finais.
- 10.1.12.31. O agente antivírus deve proteger *Laptops*, *Desktops* e servidores em tempo real, sob demanda ou agendado para detectar, bloquear e limpar todos os vírus, *Trojans*, *Worms* e *Spyware*. No Windows o agente também deve detectar PUA, *Adware*, comportamento suspeito, controle de aplicações e dados sensíveis. O agente ainda deve fornecer controle de dispositivos terceiros e, controle de acesso à web;
- 10.1.12.32. Possuir mecanismo contra a desinstalação do *Endpoint* pelo usuário e cada dispositivo

deve ter uma senha única;

- 10.1.12.33. Prover no *Endpoint* a solução de HIPS (*Host Intrusion Prevention System*) para a detecção automática e proteção contra comportamentos maliciosos (análise de comportamento) e deve ser atualizado diariamente;
- 10.1.12.34. Prover proteção automática contra *Web Sites* infectados e maliciosos, assim como prevenir o ataque de vulnerabilidades de *Browser* via *Web Exploits*;
- 10.1.12.35. Permitir a monitoração e o controle de dispositivos removíveis nos equipamentos dos usuários, como dispositivos USB, periféricos da própria estação de trabalho e redes sem fio;
- 10.1.12.36. O controle de dispositivos deve ser ao nível de permissão, somente leitura ou bloqueio;
- 10.1.12.37. A ferramenta de administração centralizada deve gerenciar todos os componentes da proteção para estações de trabalho e servidores e deve ser projetada para a fácil administração, supervisão e elaboração de relatórios dos *Endpoint* e servidores;
- 10.1.12.38. Possuir interface gráfica *Web*, com suporte a língua portuguesa (padrão brasileiro);
- 10.1.12.39. A Console de administração deve incluir um painel com um resumo visual em tempo real para verificação do *Status* de segurança;
- 10.1.12.40. Fornecer filtros pré-construídos que permitam visualizar e corrigir apenas os computadores que precisam de atenção;
- 10.1.12.41. Exibir os PCs gerenciados de acordo com critérios da categoria (detalhes do estado do computador, detalhes sobre a atualização, detalhes de avisos e erros, detalhes do antivírus etc.), e classificar os PCs em conformidade;
- 10.1.12.42. Uma vez que um problema seja identificado, permitir corrigir os problemas remotamente, com no mínimo as opções abaixo:
 - a) Proteger o dispositivo com a opção de início de uma varredura;
 - b) Forçar uma atualização naquele momento;
 - c) Ver os detalhes dos eventos ocorridos;
 - d) Executar verificação completa do sistema;
 - e) Forçar o cumprimento de uma nova política de segurança;
 - f) Mover o computador para outro grupo;
 - g) Apagar o computador da lista.
- 10.1.12.43. Atualizar a políticas de segurança quando um computador for movido de um grupo para outro manualmente ou automaticamente;

- 10.1.12.44. Permitir exportar o relatório de *Logs* de auditoria nos formatos CSV e PDF;
- 10.1.12.45. Deve conter vários relatórios para análise e controle dos usuários e *Endpoints*. Os relatórios deverão ser divididos, no mínimo, em relatórios de: eventos, usuários, controle de aplicativos, periféricos e *Web*, indicando todas as funções solicitadas para os *Endpoints*;
- 10.1.12.46. Fornecer relatórios utilizando listas ou gráficos, utilizando informações presentes na console, com no mínimo os seguintes tipos:
- a) Nome do dispositivo;
 - b) Início da proteção;
 - c) Último usuário logado no dispositivo;
 - d) Último *Update*;
 - e) Último escaneamento realizado;
 - f) *Status* de proteção do dispositivo;
 - g) Grupo a qual o dispositivo faz parte;
- 10.1.12.47. Permitir a execução manual de todos estes relatórios nos formatos CSV e PDF;
- 10.2. PROCESSO DE EXECUÇÃO DO SERVIÇO MONITORAMENTO, DETECÇÃO E RESPOSTA A INCIDENTES PARA ENDPOINTS**
- 10.2.1. O gerenciamento da solução de segurança Endpoint Security deverá contemplar as atividades listadas abaixo.
- 10.2.1.1. Administração da solução de Endpoint Security seguindo as melhores práticas do fabricante da solução;
 - 10.2.1.2. Configuração da console de gerência;
 - 10.2.1.3. Realizar health check mensal na plataforma para otimizar configurações de forma corretiva ou preventiva visando a redução de riscos de segurança e elevação do nível de maturidade;
 - 10.2.1.4. Instalar, configurar e documentar novos componentes ou novas funcionalidades que estiverem disponíveis no produto;
 - 10.2.1.5. Customizar relatórios nativos a partir da solução de gerência da solução de Endpoint Security;
 - 10.2.1.6. Instalação remota dos agentes nos dispositivos (servidores e desktops e notebooks).
 - 10.2.1.7. Identificar e corrigir de forma proativa ou corretiva problemas na eficácia do endpoint

gerenciado;

- 10.2.1.8. Integrar a solução com o ambiente do cliente utilizando integrações nativas que não dependam de desenvolvimento, como por exemplo, autenticação LDAP, envio de alertas de e-mails via relay;
- 10.2.1.9. Configurar alertas e notificações na plataforma, conforme alinhamento com o cliente;
- 10.2.1.10. Corrigir falhas e problemas que impactem nas funcionalidades ou disponibilidade da aplicação que não dependam diretamente da infraestrutura local como acesso à internet, falhas de comunicação decorrentes de falhas de rede, falhas no sistema de virtualização etc.;
- 10.2.1.11. Notificar o cliente sempre que houver novas versões do produto, elaborar documento de implantação para execução do upgrade e realizar upgrade da solução após aprovação formal do cliente;
- 10.2.1.12. Apoiar na criação das rotinas de backup e restore da solução em casos de desastres seguindo as recomendações e melhores práticas do fabricante da solução;
- 10.2.1.13. Em casos de incidentes de segurança que impactem o funcionamento da solução de Endpoint Security a CONTRATADA deverá apoiar na reconstrução do ambiente administrado por este contrato;
- 10.2.1.14. Atender a requisições de serviço que tratem de dúvidas sobre funcionalidade ou configurações do produto adquirido neste contrato;
- 10.2.1.15. Realizar reuniões mensais para acompanhamento dos resultados;
- 10.2.1.16. Acionar equipe de Segurança da Informação da CONTRATANTE para auxiliar em diagnóstico e tratamento de problemas de maior complexidade e impacto;
- 10.2.1.17. Certificar diariamente que as atualizações de vacinas estejam sendo recebidas e distribuídas para o parque de ativos;
- 10.2.1.18. Definir e manter atualizado os procedimentos operacionais relacionados a solução listados abaixo.
 - 10.2.1.18.1. Troubleshooting de comunicação.
 - 10.2.1.18.2. Troubleshooting de vacinas.
 - 10.2.1.18.3. Troubleshooting de funcionamento do agente.
 - 10.2.1.18.4. Procedimento de instalação do agent.
 - 10.2.1.18.5. Tratamento de incidentes relacionados a solução de Endpoint Security.

10.2.2. ENTREGAS A SEREM REALIZADAS

10.2.2.1. Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, o CONTRATANTE definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue de forma on line e em tempo de execução, através do portal de indicadores descrito no tópico de condições gerais para prestação do serviço deste termo de referência, a saber:

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Ameaças identificadas na solução de endpoint Security	Soma de ameaças	Ameaças	Ameaças	Número total de Ameaças
Conformidade de assinaturas nos endpoints gerenciados	Soma de não conformidade	Tipos com maior frequência	Conformidade	Número total de não conformidade por tipo
Cobertura de proteção dos endpoints descoberto vs instalado	Soma de divergência	Protegido	Protegidos	% do parque protegido

Tabela 6 - Indicadores Estratégicos de Monitoramento de EndPoints

11. DO PAGAMENTO DOS SERVIÇOS

- 11.1. A prestação dos serviços será baseada no modelo de remuneração em função dos resultados apresentados, em que os pagamentos serão feitos após mensuração do Nível Mínimo de Serviço (NMS) definido em contrato/Termo de Referência, de modo a resguardar a eficiência e a qualidade na prestação dos serviços.
- 11.2. O CRCMG efetuará o pagamento em até 10 (dez) dias úteis, contados a partir do recebimento da Nota Fiscal com as devidas deduções legais.
- 11.2.1. Os pagamentos terão início somente após a instalação da solução e a completa disponibilização dos serviços, mediante o aceite definitivo da CONTRATANTE.
- 11.2.2. Considera-se ocorrido o recebimento da nota fiscal ou fatura no momento em que o CRCMG contratante atestar a execução do objeto do contrato.
- 11.2.3. A Nota Fiscal deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da Lei nº 8.666, de 1993.

- 11.3. Serão descontados sobre o pagamento a ser realizado, as devidas retenções de tributos e contribuições, conforme determina a Instrução Normativa nº. 1.234, de 11/01/2012, da Secretaria da Receita Federal.
- 11.4. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para o CRCMG.
- 11.5. Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.
- 11.6. Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do CRCMG.
- 11.7. Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018.
- 11.8. Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.
- 11.9. Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.
- 11.10. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.
- 11.11. Será rescindido o contrato em execução com a contratada inadimplente no SICAF, salvo por motivo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante.
- 11.12. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

$EM = I \times N \times VP$, sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

$$I = (TX) \quad I = \frac{(6 / 100)}{365} \quad TX = \text{Percentual da taxa anual} = 6\% \\ I = 0,00016438$$

11.13. Os preços são fixos e irrevogáveis no prazo de um ano contado da data limite para a apresentação das propostas.

11.14. Dentro do prazo de vigência do contrato e mediante solicitação da contratada, os preços contratados poderão sofrer reajuste após o interregno de um ano, aplicando-se o índice IPCA acumulado nos 12 (doze) meses anteriores a data base ou outro índice que venha a substituí-lo, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

11.15. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

12. DA MENSURAÇÃO

12.1. O pagamento será feito mensalmente, levando-se em consideração o Nível Mínimo de Serviço (NMS) acordado em contrato, para o período de faturamento avaliado. O valor a ser pago será o valor unitário do item correspondente, alinhado com o NMS previsto em contrato.

12.2. Conforme ACORDO DE NÍVEIS DE SERVIÇO os SERVIÇOS GERENCIADOS DE SEGURANÇA serão medidos, nos seguintes termos:

12.2.1. DISPONIBILIDADE MENSAL DOS GRUPOS DE TECNOLOGIAS: Acompanha a execução do SERVIÇO DE GESTÃO DE DISPONIBILIDADE sobre os ativos de segurança, sob responsabilidade da CONTRATADA.

12.2.2. As qualificações técnicas exigidas para o perfil de analista(s) que participará do supracitado GRUPO DE DISPONIBILIDADE, da CONTRATADA:

Perfis	Certificações	Descrição
Analista de Segurança I	- ITIL foundation V3 - Ou - ISFS (Information Security Foundation)	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento pleno em segurança da informação, realizando monitoramento de disponibilidade de ambiente de segurança da informação, similares ao ambiente supracitado. Experiência comprovada de no mínimo 12 (doze) meses em tecnologia da informação.

Tabela 7 – Qualificações Grupo de Disponibilidade

12.2.3. No momento da assinatura do contrato, será exigido da CONTRATADA, a apresentação das documentações do(s) profissionais que participarão do GRUPO DE DISPONIBILIDADE, as quais devem comprovar as exigências e obrigações descritas neste termo de referência: contrato de prestação de serviços ou carteira de trabalho devidamente assinada pela CONTRATADA, para comprovação de habilidades, e as devidas certificações técnicas para comprovação do conhecimento conforme TABELA de exigências de qualificações.

12.2.4. ENTREGA MENSAL DOS SERVIÇOS:

12.2.4.1. Acompanha a execução de todos os demais serviços que compõem o objeto SERVIÇOS GERENCIADOS DE SEGURANÇA, sobre os ativos de segurança sob responsabilidade da CONTRATADA.

TIPO DE PRIORIDADE	QUANTIDADE DE ATENDIMENTO REALIZADO NO PERÍODO	QUANTIDADE DE ATENDIMENTO DESACORDO COM O NMS	FATOR DE ABATIMENTO POR DESEMPENHO DE SERVIÇO
P1			
P2			
P3			
P4			
P5			
P6			
P7			
P8			
VTAD (Valor R\$ total apurado)			

Tabela 8 – Dashboard de entrega de serviços

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR
Tipo de prioridade	N/A	N/A	N/A
Quantidade de atendimento realizado no período	Soma de todos os atendimentos realizados no período	Período de apuração	Prioridade
Quantidade de atendimento desacordo com o NMS	Soma de todos os atendimentos realizados no período que não estão em conformidade com o NMS supracitado	Período de apuração	Prioridade
Fator de abatimento por desempenho de serviço (FADS)	Conforme item ENTREGA MENSAL DOS SERVIÇOS	Período de apuração	Prioridade

	GERENCIADOS DE SEGURANÇA		
VTAD (Valor R\$ total apurado)	Soma do total de FADS, e subtrai do valor total previsto para o período	Período apuração de	N/A

Tabela 9 – Legenda de entrega de serviços

- 12.3. A reunião mensal deverá ocorrer até o 5º (quinto) dia útil após o término do período de faturamento, que coincidirá com o mês legal, e a disponibilidade dos relatórios será condição necessária ao recebimento dos serviços pelo CONTRATANTE. O primeiro mês de faturamento será parcial e proporcional, contado da data da emissão do termo de recebimento definitivo até o último dia do mês. Neste contexto, o profissional deve apresentá-lo de forma virtual, por meio de solução de videoconferência.
- 12.4. A respectiva nota fiscal/fatura, já deduzidos os fatores de abatimento calculados, deverá ser emitida somente após o recebimento definitivo dos serviços, e após a homologação das informações apresentadas pela CONTRATADA ao CONTRATANTE.
- 12.5. Caso não haja concordância da CONTRATADA com os fatores de abatimento calculados, os mesmos serão convertidos em sanção, aplicação de multa de mesmo valor, de forma a garantir o contraditório e a ampla defesa.
- 12.6. A qualquer tempo e a critério do CONTRATANTE, a bases dos sistemas utilizados para cálculo das entregas e indicadores listados neste tópico poderão ser solicitadas para auditorias e aferições.

13. DA ABRANGÊNCIA E ESCOPO DOS SERVIÇOS:

- 13.1. Considerar-se-á, para efeitos desta contratação, todos os recursos necessários para a perfeita execução efetiva da prestação dos serviços.
- 13.2. O dimensionamento da equipe para a execução adequada do serviço contratado é de responsabilidade exclusiva da CONTRATADA, devendo ser suficiente para o cumprimento integral dos níveis de serviço exigidos neste Termo de Referência.
- 13.3. Dependendo da complexidade, criticidade e do prazo do projeto, os serviços poderão ser realizados nas instalações da CONTRATADA ou da CONTRATANTE.
- 13.4. Todos os custos com licenças de simuladores, *Softwares* devem estar contabilizados no valor do serviço, não sendo permitido o pagamento de valores adicionais ou extras, seja a que título for.

14. EXECUÇÃO DOS SERVIÇOS

- 14.1. A contratada deverá cumprir o seguinte cronograma de implantação dos serviços:

CRONOGRAMA DE IMPLANTAÇÃO

ITENS	SERVIÇOS PREVISTOS:	PRAZO
1	Reunião de início de projeto (Kick-Off). Deverá ser previamente agendada pela CONTRATADA com até 02 (dois) dias úteis de antecedência.	10*
2	Entrega do Projeto Executivo pela CONTRATADA , a partir da reunião de início do projeto (Kick-Off).	30*
3	Manifestação de reajustes pela CONTRATANTE , se for o caso, a partir da data de entrega do Projeto Executivo.	10*
4	Ajustes, se for o caso, no Projeto Executivo pela CONTRATADA , a partir da manifestação de reajustes pela CONTRATANTE .	10*
5	Centro de Operações de Segurança da CONTRATADA em pleno funcionamento e operação em regime 24x7x365, a partir da data de início da vigência do contrato.	75*
6	Conclusão da fase de implantação dos serviços, contados a partir da data de início da vigência do contrato. Após a emissão do termo de recebimento definitivo pela CONTRATANTE .	90*
7	Disponibilidade dos serviços pela CONTRATADA .	60 meses**

Tabela 10 – Cronograma de implantação

* Prazos em dias corridos contados da data de assinatura do contrato.

** Prazo em meses contado a partir da assinatura do contrato.

14.2. A **CONTRATADA** deverá atender às seguintes condições gerais para início da prestação de cada um dos serviços, incluindo fase de concepção da solução, confecção de Projeto Executivo, planejamento de atividades de instalação, customização de ambiente e ativação de serviços sem ônus adicionais ao **CONTRATANTE**:

14.2.1. Reunião de início do projeto (*Kick-Off*), a ser realizada em até 10 (dez) dias corridos após a assinatura do contrato, a ser previamente agendada pela **CONTRATADA** com 02 (dois) dias úteis de antecedência.

14.2.1.1. A reunião deverá ser realizada preferencialmente de forma remota.

14.2.2. Serão de responsabilidade da **CONTRATADA** as atividades de instalação, integração, configuração e testes de todos os produtos componentes de cada solução alocada, excluindo-se a Solução de Segurança da **CONTRATANTE** já ativa (Firewall), em conformidade com o Projeto Executivo a ser elaborado e apresentado pela **CONTRATADA** para prévia aprovação pela **CONTRATANTE**;

14.2.3. A **CONTRATADA** deverá levantar informações acerca dos locais de instalação dos produtos durante a elaboração do Projeto Executivo, e, se necessário, efetuar visita técnica para verificar eventuais requisitos físicos a serem providos para a correta instalação e prestação dos serviços;

14.2.4. A elaboração do Projeto Executivo é de responsabilidade da **CONTRATADA** e deverá conter as fases do projeto, os cronogramas de execução, e a descrição detalhada dos produtos e subprodutos a serem entregues em cada fase.

- 14.2.4.1. A conclusão da fase de implantação dos serviços é de até 90 (noventa) dias corridos, contados a partir da data de assinatura do contrato, iniciando-se, a partir de então, a fase de prestação mensal dos serviços, apenas após a emissão do termo de recebimento definitivo.
- 14.2.5. Conter a descrição de topologia lógico e física da rede atual e topologia pretendida em cada etapa;
- 14.2.6. Efetuar o mapeamento de criticidade de todos os ativos envolvidos no projeto, inclusive os de propriedade da CONTRATANTE;
- 14.2.7. Para a implantação dos serviços, indicar de forma detalhada as condições de *Rollback* de cada mudança no ambiente da CONTRATANTE;
- 14.2.8. Estimar o consumo de Unidades de *Rack* (U) e de energia de cada ativo a ser instalado nas dependências da CONTRATANTE, se for o caso;
- 14.3. Os *Softwares* e demais componentes necessários à correta prestação dos serviços deverão:
 - 14.3.1. Conter os recursos necessários e estarem configurados de modo a garantir total operabilidade no ambiente computacional da CONTRATANTE e otimizados para usufruir das melhores condições em termos de desempenho e disponibilidade;
 - 14.3.2. Conter a última versão de *Software* e *Firmware* homologado pelo fabricante;
 - 14.3.3. Ter configuradas senhas de acesso para que a equipe de funcionários designados pelo CONTRATANTE efetue o acesso para a visualização das configurações e *Logs* (acesso seguro e remoto);
 - 14.3.4. Ter configurada senha com direitos totais de administração e configuração a ser utilizada pela CONTRATANTE em caso de emergência;
- 14.4. Para aprovação da instalação e configuração de qualquer item que ensejar a emissão de termo de recebimento definitivo, a CONTRATADA deve elaborar relatório técnico com análise dos resultados e impactos decorrentes da atividade executada;
- 14.5. Quando realizadas no ambiente de produção, as atividades poderão ser agendadas para serem executadas após o horário de expediente, a saber, em horários noturnos – após às 20h00 (vinte horas) – além de finais de semana e feriados, conforme disponibilidade da CONTRATANTE;
- 14.6. A operação assistida deverá obedecer aos requisitos a seguir:
 - 14.6.1. Iniciará quando forem finalizados o planejamento, a customização de ambiente e a instalação dos ativos de rede, sendo o item de serviço submetido para recebimento definitivo.
 - 14.6.2. A mudança para o ambiente de produção será concomitante a este momento, salvo se expressamente solicitado pela CONTRATANTE que seja feita em data diferente. Terá duração

de até 30 (trinta) dias corridos, e será executada em Belo Horizonte-MG, nas dependências da CONTRATANTE, em horário comercial (entre 8h30 e 17h30);

- 14.6.3. Caso seja necessária a consecução de atividades pelo técnico responsável pela operação assistida, e que possa afetar a disponibilidade de serviços do ambiente da CONTRATANTE, estas deverão ocorrer após às 20h00 (vinte) horas;
- 14.7. Caso a CONTRATANTE encontre pendências impeditivas à emissão do termo de recebimento definitivo, a operação assistida deverá ser prorrogada até que sejam sanados os motivos geradores das pendências;
- 14.8. Caso a implantação de um serviço cause interferência no funcionamento de qualquer funcionalidade na CONTRATANTE, a CONTRATADA deverá alocar profissionais com qualificação suficiente para corrigir o problema ou retornar o ambiente à condição anterior à implantação, sem quaisquer custos adicionais a CONTRATANTE.
- 14.9. Para todos os componentes da solução, a CONTRATADA deverá implementar e documentar as respectivas configurações de segurança necessárias, que visem à redução do risco de acesso indevido a cada servidor (*Hardening*), como, por exemplo, remoção de serviços desnecessários do sistema operacional, configurações de *Kernel*, configurações dos serviços ativos para suas permissões mínimas de funcionamento, remoção de usuários padrão de sistemas e aplicativos, além de eventuais configurações para resistir a ataques de negação de serviço.
- 14.10. Para o planejamento e o acompanhamento da instalação dos *Softwares* necessários à execução dos serviços, da entrega das etapas para recebimento definitivo, da confecção do Projeto Executivo, da confecção do as-built, e para as demais atividades pertinentes até a emissão do termo de recebimento definitivo de todos os itens, a CONTRATADA deverá alocar GERENTES DE PROJETOS.
- 14.11. As qualificações técnicas mínimas exigidas para o perfil de GERENTE DE PROJETO da CONTRATADA são:

Certificações	Descrição
Ao menos uma das certificações de segurança da informação: • Project Management Professional (PMP); • Prince2 Practitioner Certificate in Project Management; • Professional Scrum Master I;	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em gerencia de projetos, com experiência mínima de 12 (doze) meses.

Tabela 11 – Qualificações do Gerente de Projeto

- 14.11.1. **No momento da assinatura do contrato** será exigido da CONTRATADA a apresentação das documentações do(s) profissional(is) com perfil de GERENTE DE PROJETO, as quais devem comprovar as exigências e obrigações descritas neste Termo de Referência: contrato de prestação de serviços ou carteira de trabalho devidamente assinada pela CONTRATADA, para comprovação de habilidades, e as devidas certificações técnicas para comprovação do conhecimento conforme TABELA de exigências de qualificações.

15. ACORDO DE NÍVEIS DE SERVIÇO

- 15.1. A prestação dos serviços será baseada no modelo de remuneração em função dos resultados apresentados, em que os pagamentos serão feitos após mensuração e verificação de métricas quantitativas e qualitativas, contendo indicadores de desempenho e metas, com Nível Mínimo de Serviço (NMS) definido em contrato, de modo a resguardar a eficiência e a qualidade da prestação dos serviços.
- 15.2. Os níveis mínimos de serviço contratados serão registrados, monitorados e comparados às metas de desempenho e qualidade estabelecidas, em termos de prazo e efetividade, condição fundamental para realização dos pagamentos previstos.
- 15.3. De modo a facilitar a compreensão dos Níveis Mínimos de Serviço (NMS) dos Serviços Gerenciados de Segurança, são apresentadas, a seguir, exigências mínimas em termos de níveis de serviço que devem ser atendidas pela CONTRATADA na execução do contrato, a saber:
- 15.4. **DISPONIBILIDADE MENSAL DOS GRUPOS DE TECNOLOGIAS**
- 15.4.1. Para os itens 1 a 5 dos Serviços Gerenciados de Segurança, a Meta de Disponibilidade Mensal (MDM) por grupo de tecnologia deve ser de, no mínimo:

item	Grupo de Tecnologia	MDM (%)	FPI
1	Proteção de Dados e <i>Datacenter</i>	95	1,75
2	Proteção de Dados de <i>Endpoints</i>	95	1,5
4	Visibilidade de Rede e Controle de Incidentes	95	1,5

Tabela 12 – Meta de Disponibilidade Mensal

- 15.5. O SERVIÇO DE GESTÃO DE DISPONIBILIDADE foi arquitetado para garantir e medir a disponibilidade do parque de segurança da informação descrito neste Termo de Referência. Logo, o mesmo deverá ser utilizado para apurar a meta de disponibilidade mensal (MDM).
- 15.6. Em cada período avaliado, o cálculo do Percentual de Disponibilidade Mensal (PDM) por item de serviço deve ser calculado com a seguinte fórmula:

$$PDM_k = \frac{[TM - TI_k]}{TM} * 100$$

PDM_k = Percentual de Disponibilidade Mensal do k-ésimo item de serviço;
 k = k-ésimo item de serviço;

TM = Tempo total mensal de operação, em minutos, no mês de faturamento;

TI_k = Tempo total mensal de indisponibilidade do k-ésimo item de serviço, em minutos, no mês de faturamento.

Devem ser incluídos como Tempo de Indisponibilidade (TI_k):

- 15.7. Tempo em que o respectivo serviço esteja indisponível ou com desempenho degradado;
- 15.8. Tempo decorrente entre o início da indisponibilidade do serviço e a sua total recuperação;
- 15.9. Não devem ser incluídos como Tempo de Indisponibilidade (TI_k):
 - 15.9.1. Falta de energia no local de prestação dos serviços;
 - 15.9.2. Indisponibilidade da rede lógica da CONTRATANTE;
 - 15.9.3. Problemas derivados de ocorrências no ambiente da CONTRATANTE, onde comprovadamente a indisponibilidade não esteja sendo controlada pela CONTRATADA;
 - 15.9.4. Ações necessárias para resolução de problemas que tenham sido autorizadas pelo CONTRATANTE;
 - 15.9.5. Indisponibilidade gerada pela operadora de telecomunicação responsável pelos *Links* e equipamentos do ambiente da CONTRATANTE;
 - 15.9.6. Fatores externos a prestação de serviços, desde que justificado e acordado com o time de segurança da CONTRATANTE;
 - 15.9.7. Indisponibilidade do ambiente virtualizado da CONTRATANTE, infraestrutura computacional em que parte dos *Softwares* que compõem a solução deve ser instalada;
 - 15.9.8. Manutenções programadas pela CONTRATANTE;
 - 15.9.9. Manutenções programadas pela CONTRATADA, desde que previamente autorizadas pela CONTRATANTE.
 - 15.9.10. *Tickets* abertos cujo prazo de resolução encerre somente no próximo período de faturamento somente terão calculados os fatores de abatimento a partir do período seguinte;
- 15.10. Os fatores de abatimento por indisponibilidade de serviços (FAIS) relativos ao percentual de disponibilidade mensal deverão, ainda, ser multiplicados por um fator de peso do item (FPI), segundo a **Tabela** - META DE DISPONIBILIDADE MENSAL, por grupo de tecnologia.
- 15.11. O Percentual de Disponibilidade Mensal (PDM) é subsidiário para o cálculo do Fator de Abatimento por Indisponibilidade de Serviço (FAIS), desconto a ser aplicado no valor de prestação mensal de cada conjunto ou item de serviço;
- 15.12. Assim sendo, o Fator de Abatimento por Indisponibilidade de Serviço (FAIS) deve ser calculado de acordo com a seguinte fórmula:

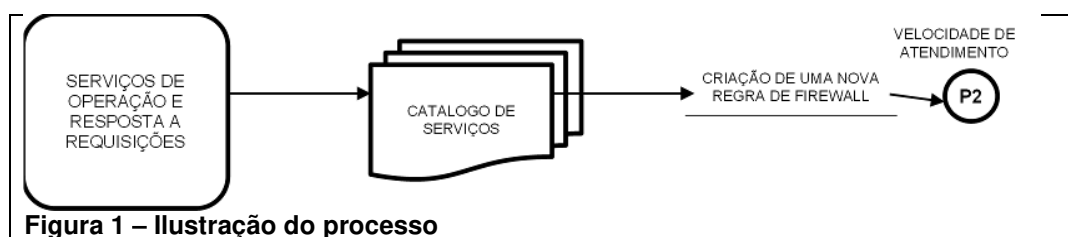
$$FAIS = \sum_{k=1}^{10} VMI_k \times FPI_k \times \left\{ \frac{MDM_k - \min(MDM_k, PD_k)}{100} \times MTI \right\}$$

Variável	Descrição
k	Número do grupo de tecnologia
FAIS	Fator de abatimento por indisponibilidade de serviço
VMI	Valor mensal do item de serviço de Gestão de Disponibilidade
MDM	Meta de disponibilidade mensal do item
PD	Percentual de disponibilidade mensal, calculada segundo fórmula supracitada.
MTI	Multiplicador por tempo de indisponibilidade, conforme definido a seguir: Valor = 1, se (MDM - PD) menor igual 1; Valor = 1, se (MDM - PD) maior que 1 e menor igual a 5; Valor = 1, se (MDM - PD) for maior que 5;
Min	Função que retorna o valor mínimo.

Tabela 13 – Variáveis de Cálculo de Fator de Abatimento por Indisponibilidade de Serviço (FAIS)

15.13. ENTREGA MENSAL DOS SERVIÇOS GERENCIADOS DE SEGURANÇA

- 15.13.1. Além da meta de disponibilidade mensal do parque de segurança da informação do CONTRATANTE, a qual avalia especificamente o **SERVIÇO DE GESTÃO DE DISPONIBILIDADE**, também deverão ser apurados os níveis de serviço para os demais serviços que, somados, compõem o objeto Serviços Gerenciados de Segurança.
- 15.13.2. Todos os serviços que compõem o objeto contratado possuem catálogo de serviço descrito no **ANEXO IV** deste Termo de Referência. Cada item (serviço) que compõe o catálogo de serviço deve estar relacionado com os tipos de velocidade de atendimento descritos na **Tabela 3** deste termo de referência, conforme exemplo ilustrado na figura abaixo:



Tipos	Nível mínimo de serviço (NMS)	IndMeta	Fator de peso da Atividade (FAT)
P1	2 Horas	2 Horas	1
P2	4 Horas	4 Horas	1
P3	8 Horas	8 Horas	0,5
P4	16 Horas	16 Horas	0,5
P5	32 Horas	32 Horas	0,5

P6	64 Horas	64 Horas	0,25
P7	128 Horas	128 Horas	0,25
P8	256 Horas	256 Horas	0,25

Tabela 14 – Níveis de prioridade de Atendimento

- 15.13.3. Em um atendimento onde seja necessária uma janela para execução dos serviços solicitados, o tempo transcorrido entre a necessidade do atendimento e a janela de execução deverão ser excluídos.
- 15.13.4. Os fatores de abatimento por desempenho de serviço (FADS) serão calculados com base na comparação dos resultados alcançados na execução das atividades com os níveis de serviços definidos na TABELA 14 - NIVEIS DE PRIORIDADES DE ATENDIMENTO.
- 15.13.5. O FADS será calculado como somatório das ocorrências realizadas para cada uma das atividades definidas, conforme fórmula a seguir:

$$FADS = \sum_{i=1}^8 \sum_{j=1}^n VMC \times \left[\frac{\text{Max} (INDATINGi.j, INDMETAi) - INDMETAi}{10 \times INDMETAi} \right] \times FPAi$$

Variável	Descrição
I	Tipo de prioridade.
J	Contador de ocorrências do tipo de prioridade que não atenderam o NMS definido.
N	Quantidade de ocorrências do tipo de prioridade que não atenderam o NMS definido.
FADS	Fator de abatimento por desempenho de Serviço
VMC	Valor mensal do contrato.
INDMETA	Índice de meta (NMS), em minutos/horas/dias, definido para a atividade.
INDATING	Índice atingido, em minutos/horas/dias, pela atividade que ultrapassou o (NMS).
FPA	Fator de peso da atividade.
Max	Função que retorna o valor máximo.

Tabela 15 – Variáveis de Cálculo de Fatores de Abatimento por Desempenho de Serviço (FADS)

16. PAPÉIS E RESPONSABILIDADES

- 16.1. Durante a vigência contratual, e toda a prestação do serviço objeto desta contratação, deverão ser observados e cumpridos os seguintes papéis e responsabilidades dos profissionais:
- 16.1.1. **Fiscal técnico do contrato (CONTRATANTE):** responsável pelo acompanhamento, fiscalização e avaliação da execução do objeto nos moldes contratados, observando o fiel cumprimento de todas as cláusulas contratuais.
- 16.1.2. **Gestor do contrato (CONTRATANTE):** responsável pela coordenação das atividades relacionadas à fiscalização, bem como dos atos preparatórios à instrução processual e da

formalização dos procedimentos referentes aos aspectos que envolvam a prorrogação, a alteração, o reequilíbrio, o pagamento, eventuais aplicações de sanções e extinção dos contratos, dentre outras ações.

- 16.1.3. **Preposto (CONTRATADA):** é o profissional indicado pelo Fornecedor de Serviço para representá-la administrativa e tecnicamente. É o responsável pela coordenação operacional das atividades previstas nos projetos, de forma a solucionar qualquer dúvida, conflito ou desvio técnico que possa comprometer a execução das OS. Deverá ter bons conhecimentos em gestão de projetos para garantir o controle sobre os sinais vitais de cada projeto. Também é responsável pela interlocução com o Gestor do Contrato do CONTRATANTE.

16.2. As qualificações técnicas exigidas para o perfil de PREPOSTO da CONTRATADA:

Certificações	Descrição
Ao menos uma das certificações de segurança da informação: • CISSP (Certified Information Systems Security Professional); • CISM (Certified Information Security Manager); • CIA (Certified Intrusion Analyst), • GSEC (GIAC Security Essentials); • GCIH (GIAC Incident Handler) • GMON (GIAC Continuous Monitoring);	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência mínima de 12 (doze) meses em coordenação e gestão de contratos de serviços continuados.

Tabela 16 – Certificações e Qualificações do Preposto

- 16.3. **No momento da assinatura do contrato** será exigido da CONTRATADA a apresentação das documentações do(s) profissionais com perfil de PREPOSTO as quais devem comprovar as exigências e obrigações descritas neste termo de referência: contrato de prestação de serviços ou carteira de trabalho devidamente assinada pela CONTRATADA para comprovação de habilidades e as devidas certificações técnicas para comprovação do conhecimento conforme TABELA 16.

17. ESCOPO E PRAZOS DE EXECUÇÃO E DE ACEITE E NATUREZA DOS SERVIÇOS

- 17.1. O período de prestação dos serviços, a partir da emissão do termo de recebimento definitivo será o estabelecido na tabela abaixo:

LOTE	ITEM	DESCRIÇÃO	QTD	MÉTRICA	PERÍODO
1	1	Serviço de Monitoramento de Ataques Cibernéticos e Resposta A Incidentes	1	500 EPS*	60
	2	Serviço de Gestão de Vulnerabilidades	300	Ativos	60
	3	Serviço de Monitoramento, Detecção e Resposta a Incidentes para Endpoint	130	Ativos	60

*EPS - Eventos por Segundo - é uma métrica utilizada pelo mercado para dimensionar o SIEM (equipamento responsável pela coleta, análise e correlacionamento dos Logs).

- 17.2. SERVIÇOS GERENCIADOS DE SEGURANÇA – DEMANDA FUTURA serão demandados de acordo com as necessidades da CONTRATANTE, solicitados por meio de Ordem de Serviço cuja execução deve ser recebida por meio do Termo de Recebimento de Serviços.
- 17.3. A partir da assinatura do contrato, correrão os seguintes prazos:
- 17.4. Reunião de início do projeto (*Kick-Off*): a ser realizada em até 10 (dez) dias corridos após a assinatura do contrato. Deverá ser previamente agendada pela **CONTRATADA** com 02 (dois) dias úteis de antecedência.
- 17.5. Entrega do Projeto Executivo: até 30 (trinta) dias corridos, contados a partir da reunião de início do projeto (*Kick-Off*);
- 17.6. A CONTRATANTE se manifestará no prazo de até 10 (dez) dias corridos, contados da data de entrega do Projeto Executivo;
- 17.7. Havendo necessidade de ajustes, a CONTRATADA terá até 10 (dez) dias corridos para realizá-los, contados da notificação a ser efetuada pela CONTRATANTE, a respeito da manifestação sobre o Projeto Executivo;
- 17.8. A conclusão da fase de implantação dos serviços é de até 90 (noventa) dias corridos, contados a partir da data de início da vigência do contrato, mediante a emissão do termo de recebimento definitivo pela CONTRATANTE.
- 17.9. O termo de recebimento definitivo obedecerá os seguintes critérios:
- 17.10. A CONTRATANTE terá 15 (quinze) dias corridos para emitir o termo de recebimento definitivo depois de finalizado o planejamento, customização e a instalação do ambiente;
- 17.11. A prestação dos serviços mensais iniciará somente a partir da emissão do termo de recebimento definitivo pela CONTRATANTE;
- 17.12. Para todos os bens importados, caso necessário, por parte da CONTRATADA, que sejam instalados nas dependências da CONTRATANTE, será necessária a apresentação dos respectivos comprovantes de origem.
- 17.13. O Centro de Operações de Segurança da CONTRATADA deverão estar em pleno funcionamento, operando em regime 24x7x365, em até 75 (setenta e cinco) dias corridos, contados da data de início da vigência contratual.

18. INSPEÇÕES E DILIGÊNCIAS

- 18.1. A CONTRATANTE reserva-se o direito de efetuar inspeções e diligências para sanar quaisquer dúvidas existentes, podendo efetuá-las previamente à contratação;

- 18.2. A CONTRATANTE poderá realizar diligência no Centro de Operações de Segurança da CONTRATADA antes do início da prestação do serviço, *in loco*, a fim de validar e aferir se TODOS os itens solicitados neste Termo de Referência serão atendidos;
- 18.3. A contratação não será formalizada, caso **não** haja o atendimento de quaisquer itens previstos neste Termo de Referência.
- 18.4. As Diligências não poderão ser restritas a dias e horários específicos, sendo possível que a mesma seja executada em horários fora do chamado “horário comercial”, sendo possível a visitação em finais de semana, períodos noturnos e afins;
- 18.5. A CONTRATADA poderá restringir a quantidade de pessoas presentes na diligência, porém ela deverá apresentar durante a visita todas as comprovações necessárias, todos os processos solicitados e responder a todos os questionamentos.
- 18.6. Em caso de eventos adversos que impossibilitem a diligência a contratada deverá prover acesso de maneira remota e virtual para a verificação dos itens a serem inspecionados.

19. TRATAMENTO DE INCIDENTES CIBERNÉTICOS

- 19.1. É de responsabilidade da CONTRATADA a restauração dos serviços comprometidos através da definição de estratégias e de ações para conter o incidente; a erradicação dos artefatos maliciosos do ambiente do CRCMG; a recuperação dos serviços dependentes de tecnologia; bem como ações que terão como objetivo mitigar riscos existentes para evitar com que incidentes semelhantes ocorram no futuro.
- 19.1.1. É de responsabilidade da CONTRATANTE contactar as suas terceirizadas para atendimento das estratégias e ações repassadas pela CONTRATADA para completo restabelecimento do ambiente o mais rápido e seguro.
- 19.1.1.1. Serviços de responsabilidade da CONTRATANTE:
- a) Restauração de Backups de servidores, serviços, dados, banco de dados, configurações do AD, senhas, GPOs, grupos;
 - b) Configuração do Firewall;
- 19.2. Os serviços a serem executados, culminarão na entrega pela contratada dos seguintes documentos:
- 19.2.1. **Relatório executivo** – Demonstrará a conformidade e riscos antes da aplicação dos controles de segurança e após a aplicação dos controles de segurança;
- 19.2.2. **Relatório técnico** – Demonstrará tecnicamente os controles aplicados e o nível de conformidade individual de cada estação de trabalho e servidor, abrangendo:
- 19.2.2.1. Tratamento de incidentes: ações realizadas para mitigação dos riscos;

19.2.2.2. Relatório forense: Relatório demonstrando as ações do ator de ameaça;

19.2.2.3. Principais riscos: Principais riscos identificados;

19.2.2.4. Plano Diretor: Plano de ação e recomendações para lidar com os riscos residuais;

19.3. A CONTRATADA deverá emitir relatórios técnicos e auxiliar o CRCMG na elaboração de respostas às autoridades competentes, quando necessário e a critério do CRCMG, no caso de eventual incidente de segurança da informação.

20. MODALIDADE DA LICITAÇÃO

Pregão Eletrônico.

21. VALOR DE REFERÊNCIA

21.1. O valor de referência, que corresponde ao **VALOR GLOBAL MÁXIMO** que o CRCMG se propõe a pagar pela prestação dos serviços, objeto deste Termo de Referência, pelo período de 60 (sessenta) meses é de R\$ 872.250,00 (oitocentos e setenta e dois mil duzentos e cinquenta reais).

VALOR DE REFERÊNCIA	
Estimativa Mensal	Estimativa Global 60 meses
R\$ 14.537,50	R\$ 872.250,00

21.2. No valor que vir a oferecer deverão ser incluídas todas as despesas com os profissionais e equipamentos, bem como, taxas, alimentação, transporte, hospedagem, enfim, todos os encargos fiscais, comerciais, trabalhistas e previdenciários, resultantes da prestação dos serviços objeto deste Procedimento.

22. CRITÉRIO DE JULGAMENTO DAS PROPOSTAS

22.1. No julgamento das propostas, será considerada vencedora a que apresentar **MENOR PREÇO GLOBAL**, desde que atendidas às especificações constantes deste Edital e de seus Anexos.

22.2. Será desclassificada a proposta que, para sua viabilização, apresente vantagens ou subsídios que não estejam previamente autorizados em lei, assim como as que não se encontrem em conformidade com os requisitos estabelecidos no presente Edital.

22.3. O julgamento das propostas será de acordo com a sistemática do site de compras denominado www.comprasnet.gov.br, em consonância com a legislação vigente.

23. DO PRAZO DE VIGÊNCIA DO CONTRATO

O contrato vigorará pelo prazo de 60 (sesenta) meses, a contar da data de sua assinatura e será regido pelas Leis nº 10.520/02, nº 8.666/93 e pelo Código Civil Brasileiro.

24. DA GARANTIA CONTRATUAL

- 24.1. A CONTRATADA, no prazo de até 20 (vinte) dias, contado a partir da data de assinatura deste contrato, prestará garantia de cumprimento das obrigações contratuais, correspondente a 5 % (cinco por cento) do valor estimado para a execução dos serviços, objeto deste contrato.
- 24.1.1. O prazo estipulado no subitem anterior poderá ser prorrogado por igual período, a juízo do CRCMG, à vista das justificativas que lhe forem apresentadas pela CONTRATADA.
- 24.1.2. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa, nos termos do item 25.2.4.5.
- 24.1.3. O atraso superior a 30 (trinta) dias corridos, após os prazos previstos nos subitens 24.1 e 24.1.1, autoriza a CONTRATANTE a promover a rescisão deste contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os incisos I e II do art. 78 da Lei nº 8.666/1993, sem prejuízo de outras sanções previstas na Lei e neste contrato.
- 24.2. Caberá à CONTRATADA escolher uma das modalidades previstas no art. 56 da Lei nº 8.666/1993:
- a) caução em dinheiro ou títulos da dívida pública;
 - b) seguro-garantia;
 - c) fiança bancária.
- 24.3. Em se tratando de garantia prestada por meio de caução em dinheiro, o depósito deverá ser feito obrigatoriamente na Caixa Econômica Federal, conforme determina o art. 82 do Decreto n.º 93.872/1986, em caderneta de poupança, em favor do CRCMG, e será corrigida pelos índices oficiais aplicados à essa modalidade de depósito bancário.
- 24.4. Se a opção for pelo seguro-garantia:
- a) a apólice indicará o CRCMG como beneficiário, devendo ser emitida por instituição autorizada pela Superintendência de Seguros Privados (SUSEP) a operar no mercado securitário, que não se encontre sob regime de direção fiscal, intervenção, liquidação extrajudicial ou fiscalização especial e que não esteja cumprindo penalidade de suspensão imposta pela autarquia;
 - b) seu prazo de validade deverá corresponder ao período de vigência deste contrato, acrescido de 90 (noventa) dias para apuração de eventual inadimplemento da CONTRATADA, ocorrido durante a vigência contratual, e para a comunicação da expectativa de sinistro ou do efetivo aviso de sinistro à instituição emitente, observados os prazos prescricionais pertinentes;
 - c) a apólice deve prever expressamente responsabilidade da seguradora por todas e quaisquer multas de caráter sancionatório aplicadas à CONTRATADA.

24.5. Se a opção for pela fiança bancária, o instrumento de fiança deve:

- a) ser emitido por instituição financeira que esteja autorizada pelo Banco Central do Brasil a funcionar no Brasil e que não se encontre em processo de liquidação extrajudicial ou de intervenção da autarquia;
- b) ter prazo de validade correspondente ao período de vigência deste contrato, acrescido de 90 (noventa) dias para apuração de eventual inadimplemento da CONTRATADA, ocorrido durante a vigência contratual, e para a comunicação do inadimplemento à instituição financeira, observados os prazos prescricionais pertinentes;
- c) ter afirmação expressa do fiador de que, como devedor solidário, fará o pagamento ao CRCMG, independentemente de interpelação judicial, caso o afiançado não cumpra suas obrigações;
- d) ter renúncia expressa do fiador ao benefício de ordem e aos direitos previstos nos arts. 827 e 838 do Código Civil Brasileiro.

24.6. Se a opção for pelo título da dívida pública, este deverá:

- a) ter sido emitido sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil;
- b) ser avaliado por seu valor econômico, conforme definido pelo Ministério da Economia.

24.7. A garantia, qualquer que seja a modalidade escolhida, assegurará o pagamento de:

- a) prejuízos advindos do não cumprimento do objeto deste contrato e do não adimplemento das demais obrigações nele previstas;
- b) prejuízos causados ao CRCMG ou a terceiro, decorrentes de culpa ou dolo durante a execução deste contrato;
- c) multas moratórias e punitivas aplicadas pelo CRCMG à CONTRATADA; e
- d) obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza, não adimplidas pela CONTRATADA.

24.7.1. A modalidade seguro garantia somente será aceita se contemplar todos os eventos indicados no subitem 24.7.

24.8. Não serão aceitos seguro-garantia ou fiança bancária que contenham cláusulas contrárias aos interesses do CRCMG.

24.9. Sem prejuízo das sanções previstas em lei e neste contrato, a não prestação da garantia exigida implicará sua imediata rescisão.

- 24.10. Se o valor da garantia vier a ser utilizado, total ou parcialmente, no pagamento de qualquer obrigação vinculada a este ajuste, incluída a indenização a terceiros, a CONTRATADA deverá proceder à respectiva reposição, no prazo máximo de 20 (vinte) dias, contados da data do recebimento da notificação do CRCMG.
- 24.11. Se houver acréscimo ao valor deste contrato, a CONTRATADA se obriga a fazer a complementação da garantia no prazo máximo 20 (vinte) dias, contados da data do recebimento da notificação do CRCMG.
- 24.12. Na hipótese de prorrogação deste contrato, o CRCMG exigirá nova garantia, escolhida pela CONTRATADA entre as modalidades previstas na Lei n.º 8.666/1993.
- 24.13. O documento de constituição da nova garantia deverá ser entregue ao CRCMG no prazo máximo de 20 (vinte) dias, contados da data de assinatura do respectivo termo aditivo.
- 24.14. A garantia, ou seu saldo, será liberada ou restituída, a pedido da CONTRATADA, no prazo de 90 (noventa) dias após o término do prazo de vigência deste contrato, mediante certificação, por seu gestor ou fiscal, de que os serviços foram realizados a contento e desde tenham sido cumpridas todas as obrigações aqui assumidas.
- 24.15. A qualquer tempo, mediante entendimento prévio com o CRCMG, poderá ser admitida a substituição da garantia, observadas as modalidades previstas no subitem 24.2 deste contrato.
- 24.15.1. Aceita pelo CRCMG, a substituição da garantia será registrada no processo administrativo por meio de apostilamento.

25. DAS SANÇÕES ADMINISTRATIVAS

- 25.1. Comete infração administrativa nos termos da Lei nº 10.520 de 2002 e da Lei nº 8.666/1993, a CONTRATADA que:
- 25.1.1. inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;
 - 25.1.2. ensejar o retardamento da execução do objeto;
 - 25.1.3. falhar ou fraudar na execução do contrato;
 - 25.1.4. comportar-se de modo inidôneo; ou
 - 25.1.5. cometer fraude fiscal.
- 25.2. Pela inexecução total ou parcial do objeto deste contrato ou descumprimento de obrigações, a Administração poderá aplicar à CONTRATADA as seguintes sanções:
- 25.2.1. **Advertência por escrito**, quando do não cumprimento de quaisquer das obrigações

contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado;

25.2.2. **Suspensão temporária do direito de participar de licitação e impedimento de contratar** com a Administração, pelo prazo de até 2 (dois) anos;

25.2.3. **Impedimento de licitar e contratar** com órgãos e entidades da União, com o consequente descredenciamento no SICAF pelo prazo de até 5 (cinco) anos.

25.2.4. **Multa de:**

25.2.4.1. 0,5% (cinco décimos por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, limitada a incidência a 15 (quinze) dias. Após o décimo quinto dia e a critério da Administração, no caso de entrega com atraso, poderá ocorrer a não aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença;

25.2.4.2. 10% (dez por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;

25.2.4.3. em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida;

25.2.4.4. 3% (três por cento), 5% (cinco por cento) ou 10% (dez por cento), sobre o valor total da contratação, em caso de descumprimento de obrigações assumidas, por ocorrência, conforme a gradação estabelecida nos subitens e tabela abaixo.

25.2.4.5. 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso na apresentação da garantia (seja para reforço ou por ocasião de prorrogação), observado o máximo de 2% (dois por cento). O atraso superior a 25 (vinte e cinco) dias autorizará a Administração CONTRATANTE a promover a rescisão do contrato;

25.3. Na aplicação das sanções, o CRCMG levará em consideração a efetiva gravidade da conduta do infrator, o caráter educativo da pena, bem como, o real dano causado ao Conselho. Sendo assim, as multas e outras sanções aplicadas só poderão ser relevadas, motivadamente, por conveniência administrativa.

25.4. As FALTAS LEVES serão puníveis com a aplicação da penalidade de advertência e/ou multa, no percentual de 3% (três por cento), caracterizando-se pelo descumprimento parcial de deveres de pequena monta, assim entendidas como aquelas que não acarretam prejuízos relevantes aos serviços da Administração e a despeito delas, a regular prestação dos serviços não fica inviabilizada.

25.5. As FALTAS MÉDIAS serão puníveis com a aplicação da penalidade de multa no percentual de 5% (cinco por cento), caracterizando-se pela recorrência de quaisquer FALTAS LEVES ou pelo descumprimento parcial ou total de obrigação que acarrete prejuízos aos objetivos da Administração, mas sem inviabilizar total ou parcialmente a execução dos serviços.

25.6. As FALTAS GRAVES serão puníveis com a aplicação das penalidades de multa no percentual de 10% (dez por cento), podendo ser aplicada cumulativamente as sanções de suspensão temporária do direito de participar em licitação e impedimento de contratar com a Administração ou impedimento de licitar e contratar com órgãos e entidades da União, caracterizando-se pela recorrência de quaisquer FALTAS MÉDIAS ou pelo descumprimento parcial ou total de obrigação que acarrete prejuízos relevantes aos objetivos da Administração, inviabilizando a execução da contratação em decorrência de conduta culposa ou dolosa da contratada.

25.7. Afim de nortear na efetiva aplicabilidade das gradações que tratam nos subitens acima, será utilizada a seguinte classificação:

TIPO DE FALTA	GRAVIDADE
Veicular qualquer tipo de publicidade acerca do Contrato, salvo se houver prévia autorização da Administração do Conselho.	LEVE
Abster-se de prestar as informações e esclarecimentos que venham a ser solicitados pelo CRCMG, atendendo às solicitações nos prazos especificados.	LEVE
Não disponibilizar uma conta de e-mail para fins de comunicação entre as partes, bem como, endereço comercial e telefone de contato ou, em caso de alteração, não comunicar prontamente ao CRCMG.	MÉDIA
Alocar, na prestação dos serviços, profissionais com formação e qualificações não adequadas ou incompatíveis com a prestação dos serviços, conforme estabelecido no Termo de Referência.	MÉDIA
Utilizar empregado sem qualificação para a execução dos serviços ou, em caso de desligamento, não proceder à pronta substituição por outro profissional com a formação e qualificações estabelecidas no Termo de Referência.	MÉDIA
Provocar, por meio de seus empregados e representantes, qualquer dano patrimonial ou à imagem e reputação do CRCMG.	MÉDIA
Não substituir, após solicitação do CRCMG, empregado que tenha conduta inconveniente ou incompatível com suas atribuições.	MÉDIA
Prestar os serviços sem obedecer estritamente às condições estabelecidas neste Termo de Referência e no Contrato pactuado.	GRAVE
Não cumprir os prazos de entrega e execução dos serviços estipulados neste Termo de Referência.	GRAVE
Não providenciar a imediata correção das deficiências apontadas pelo fiscal do Contrato, quanto à execução contratual.	GRAVE
Deixar de manter todas as condições de habilitação e qualificação que ensejaram sua contratação, durante todo o período de vigência do Contrato.	GRAVE
Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços contratados.	GRAVE

25.7.1. As faltas cometidas pela Contratada que não se enquadrarem em nenhuma das ocorrências previstas na tabela acima, serão avaliadas caso a caso, no âmbito do Processo Administrativo.

25.7.2. Ao longo do período de validade da Ata, de 12 meses, o acúmulo de condutas faltosas cometidas de forma reiterada, de mesma classificação ou não, bem como as reincidências,

ensejará a aplicação, pela administração de penalidades relacionadas às faltas de maior gravidade, considerando que, o fato de a Administração relevar qualquer falta, não implicará em novação.

- 25.8. Reserva-se ao CRCMG o direito de reter e compensar, dos pagamentos da contratada, as multas referidas nos subitens anteriores, assegurado o contraditório e a apresentação de defesa prévia, nos termos da legislação vigente.
- 25.9. As sanções previstas nos subitens 25.2.1, 25.2.2 e 25.2.3 poderão ser aplicadas à CONTRATADA cumulativamente com as multas previstas no subitem 25.2.4.
- 25.10. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:
- 25.10.1. tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;
 - 25.10.2. tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;
 - 25.10.3. demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.
- 25.11. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.
- 25.11.1. As partes concordam que o envio e o recebimento das notificações e comunicações em geral, inclusive no âmbito de processo administrativo que venha a ser instaurado, serão realizados por meio de e-mail.
- 25.12. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.
- 25.13. As penalidades serão obrigatoriamente registradas no SICAF.
- 25.14. Além das sanções acima previstas, o contrato poderá ser rescindido pelos motivos previstos nos artigos 77 a 80 da Lei nº 8.666/93.

26. OBRIGAÇÕES DA CONTRATADA

- 26.1. Prestar os serviços, objeto deste Edital, cumprindo os prazos e atendendo integralmente a todas condições e especificações estabelecidas neste Termo de Referência.
- 26.2. Entregar os serviços objeto desse Edital, obedecendo aos prazos estipulados neste Termo de Referência.

- 26.3. Arcar com todos os custos necessários à execução dos serviços, objeto deste procedimento, tais como materiais, softwares e equipamentos, alimentação, transporte, hospedagem, instalações, mão de obra e quaisquer outros que forem pertinentes ao cumprimento do objeto, em conformidade com este Termo de Referência.
- 26.4. Assumir e cumprir todas as obrigações trabalhistas previstas em legislação e normas específicas, responsabilizando-se, exclusivamente, pela remuneração, encargos sociais e previdenciários, benefícios e demais despesas referentes a seus profissionais, tendo em vista que não será estabelecido nenhum vínculo empregatício ou de responsabilidade entre os profissionais disponibilizados para a execução dos serviços contratados e o CRCMG.
- 26.5. Responsabilizar-se pela idoneidade e pelo comportamento de seus empregados, prepostos ou subordinados.
- 26.6. Utilizar, na execução dos serviços, somente profissionais especializados e, em caso de desligamento, promover a reposição do profissional por outro com a mesma formação e qualificações estabelecidas neste Termo de Referência.
- 26.7. Reparar, corrigir, remover ou substituir às suas expensas, no total ou em parte, o objeto deste procedimento em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados, no prazo de 48 (quarenta e oito) horas da notificação, sem ônus par ao CRCMG.
- 26.8. Prestar todos os esclarecimentos que forem solicitados pelo CRCMG, atendendo de imediato às solicitações de seus representantes.
- 26.9. Informar, de imediato, as alterações de endereço, de número de telefones e de e-mails.
- 26.10. Assumir inteira responsabilidade, civil, administrativa e penal por danos materiais ou pessoais causados ao CRCMG e/ou a terceiros provocados por ineficiência ou irregularidades cometidas por seus empregados, contratados ou prepostos envolvidos na execução do contrato, decorrentes de dolo ou culpa.
- 26.11. Guardar o mais absoluto sigilo em relação às informações ou documentos de qualquer natureza a que venham tomar conhecimento, respondendo, administrativa, civil e criminalmente por sua indevida divulgação e/ou incorreta ou descuidada utilização.
- 26.11.1. A CONTRATA deverá apresentar, o momento de assinatura do contrato, Termo de Confidencialidade e Sigilo do Prestador, constante do Anexo VIII do Edital.
- 26.12. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, observando a prática da boa técnica e a legislação vigente.
- 26.13. Emitir as notas fiscais com as devidas deduções legais, devendo ser apresentada, juntamente, com as certidões de regularidade junto ao FGTS, ao INSS e à Justiça do Trabalho, além da Declaração de Optante pelo Simples Nacional, se for o caso.

- 26.14. Manter, durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas neste Edital.
- 26.15. Aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até 25% (vinte e cinco por cento) do valor inicial do contrato, na forma da legislação vigente.
- 26.16. Submeter-se à fiscalização do CRCMG, na execução dos serviços, seguindo todas as orientações repassadas.

27. OBRIGAÇÕES DO CRCMG

- 27.1. Proporcionar as condições necessárias à execução dos serviços ora contratados, assim como prestar, prontamente, as informações e os esclarecimentos que venham a ser solicitados pela contratada;
- 27.2. Efetuar o pagamento à contratada, de acordo com as condições de preço e prazo estabelecidas no contrato.
- 27.3. Acompanhar e fiscalizar o andamento dos serviços, por intermédio do funcionário do CRCMG designado como Fiscal do Contrato.
- 27.4. Rejeitar, no todo ou em parte, os serviços entregues em desacordo com as obrigações assumidas pela empresa contratada.
- 27.5. Comunicar a contratada toda e qualquer ocorrência relacionada com a execução do serviço.
- 27.6. Notificar a contratada, por escrito e com antecedência, sobre multas, penalidades e quaisquer débitos de sua responsabilidade.

28. SUBCONTRATAÇÃO

Não será admitida a subcontratação do objeto licitatório.

29. ALTERAÇÃO SUBJETIVA

28.1. É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa do Contratante à continuidade do contrato.

30. RESPONSÁVEIS PELO TERMO DE REFERÊNCIA

30.1 O presente Termo de Referência foi elaborado pela Gerência de Tecnologia da Informação e pela Gerência Administrativa e Financeira (GEADF) em consonância com as disposições legais e normativas aplicáveis e com o interesse e a conveniência da Administração, sendo objeto de exame e aprovação do



Ordenador de Despesa do Conselho, e passará a integrar o processo administrativo formalizado visando à instauração do certame licitatório e a efetividade da contratação.

DATA	ASSINATURA DO GERENTE DE TECNOLOGIA DA INFORMAÇÃO
Janeiro/2023	Assinado digitalmente por: CLAUDIO MARCIO ARAUJO DA SILVA CPF: 691.116.426-53 Certificado emitido por AC SOLUTI Multipla Data: 19/01/2023 11:04:13 -03:00 
DATA	ASSINATURA DO DIRETOR-ADJUNTO DE GESTÃO OPERACIONAL
Janeiro/2023	Assinado digitalmente por: JULIO CESAR DA SILVA CPF: 890.312.706-44 Certificado emitido por AC SOLUTI Multipla v5 Data: 19/01/2023 11:39:41 -03:00 
DATA	ASSINATURA DA PRESIDENTE DO CRCMG
Janeiro/2023	Assinado digitalmente por: SUELY MARIA MARQUES DE OLIVEIRA CPF: 686.588.426-49 Certificado emitido por AC SOLUTI Multipla v5 Data: 19/01/2023 13:34:08 -03:00 

Rua Cláudio Manoel, 639 - Savassi – Belo Horizonte/MG – Cep: 30140-105
Telefone: (31) 3269-8400 - www.crcmg.org.br

91



MANIFESTO DE ASSINATURAS



Código de validação: FQC7N-95TH6-V5EEW-LJ78G

Esse documento foi assinado pelos seguintes signatários nas datas indicadas (Fuso horário de Brasília):

- ✓ CLAUDIO MARCIO ARAUJO DA SILVA (CPF 691.116.426-53) em 19/01/2023 11:04 - Assinado com certificado digital ICP-Brasil
- ✓ JULIO CESAR DA SILVA (CPF 890.312.706-44) em 19/01/2023 11:39 - Assinado com certificado digital ICP-Brasil
- ✓ SUELY MARIA MARQUES DE OLIVEIRA (CPF 686.588.426-49) em 19/01/2023 13:34 - Assinado com certificado digital ICP-Brasil

Para verificar as assinaturas, acesse o link direto de validação deste documento:

<https://assinador.crcmg.org.br/validate/FQC7N-95TH6-V5EEW-LJ78G>

Ou acesse a consulta de documentos assinados disponível no link abaixo e informe o código de validação:

<https://assinador.crcmg.org.br/validate>

PESQUISA DE PREÇOS

CONTRATAÇÕES DA ADMINISTRAÇÃO PÚBLICA

CONTRATAÇÕES DE ÓRGÃOS/ENTIDADES PESQUISADOS:

- **CONSELHO FEDERAL DE CONTABILIDADE;**
- **CONSELHO REGIONAL DE CONTABILIDADE DE SÃO PAULO;**
- **TRIBUNAL REGIONAL DO TRABALHO DA 17.ª REGIÃO;**
- **TRIBUNAL REGIONAL FEDERAL DA 3ª REGIÃO.**



CONSELHO FEDERAL DE CONTABILIDADE
SAUS Quadra 05, Lote 03, Bloco J, Edifício CFC, - Bairro Asa Sul, Brasília/DF, CEP 70070-920
Telefone: e Fax: @fax_unidade@ - www.cfc.org.br

CONTRATO

Processo nº 90796110000007.000028/2022-91

Unidade Gestora: CGTI

CONTRATO Nº 35/2022 QUE CELEBRAM ENTRE SI A CONSELHO FEDERAL DE CONTABILIDADE E A EMPRESA ISH TECNOLOGIA S/A.

O **CONSELHO FEDERAL DE CONTABILIDADE – CFC**, inscrito no CNPJ/MF sob o nº 33.618.570/0001-07, com endereço no SAUS Quadra 5 Bloco J Lote 3 - Edifício CFC Asa Sul - Brasília/DF, doravante denominada CONTRATANTE, por intermédio do seu Vice-Presidente Administrativo, Contador Carlos Rubens de Oliveira, e de outro lado a empresa **ISH TECNOLOGIA S/A**, inscrita no CNPJ/MF sob o nº 01.707.536/0001-04, estabelecida Rua Judith Maria Tovar Varejão, 355, Enseada do Suá, Vitória/ES, doravante denominada CONTRATADA, neste ato representada pelo seu Diretor Regional Vítor Teixeira Costa, tendo em vista o que consta no Processo nº 90796110000007.000028/2022-91 e em observância às disposições da Lei nº 8.666, de 21 de junho de 1993, e da Instrução Normativa SEGES/MP nº 5, de 26 de maio de 2017, resolvem celebrar o presente Contrato nº 35/2022, mediante as cláusulas e condições a seguir enunciadas.

1. CLÁUSULA PRIMEIRA – OBJETO

1.1. O objeto do presente instrumento é a Contratação de empresa especializada para prestação de serviços técnicos de Administração e Operação em Regime 24x7, com posto de trabalho no Ambiente de Tecnologia da Informação, em regime de 5 dias x 8 horas diárias (horário de expediente do CFC) a fim de gerenciamento do Ambiente de Tecnologia da Informação do Conselho Federal de Contabilidade (CFC) em Brasília – DF, que serão prestados nas condições estabelecidas no Termo de Referência, anexo do Edital.

1.2. Este Termo de Contrato vincula-se ao Edital do Pregão, identificado no preâmbulo, e à proposta vencedora, independentemente de transcrição, bem como no anexo deste contrato.

1.3. Objeto da contratação: Anexo I do Termo de Referência.

2. CLÁUSULA SEGUNDA – VIGÊNCIA

2.1. O prazo de vigência deste Termo de Contrato é aquele fixado no Edital, com início na data de 3/11/2022 e encerramento em 3/11/2023, podendo ser prorrogado por interesse das partes até o limite de 60 (sessenta) meses, desde que haja autorização formal da autoridade competente e seja observado o disposto no Anexo IX da IN SEGES/MP n.º 05/2017, atentando, em especial, para o cumprimento dos seguintes requisitos:

- 2.1.1. Esteja formalmente demonstrado que a forma de prestação dos serviços tem natureza continuada;
- 2.1.2. Seja juntado relatório que discorra sobre a execução do contrato, com informações de que os serviços tenham sido prestados regularmente;
- 2.1.3. Seja juntada justificativa e motivo, por escrito, de que a Administração mantém interesse na realização do serviço;
- 2.1.4. Seja comprovado que o valor do contrato permanece economicamente vantajoso para a Administração;
- 2.1.5. Haja manifestação expressa da contratada informando o interesse na prorrogação;
- 2.1.6. Seja comprovado que a contratada mantém as condições iniciais de habilitação.
- 2.2. A CONTRATADA não tem direito subjetivo à prorrogação contratual.
- 2.3. A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo.

3. CLÁUSULA TERCEIRA – PREÇO

3.1. O valor mensal da contratação é de R\$ 66.099,92 (sessenta e seis mil noventa e nove reais e noventa e dois centavos), perfazendo o valor total anual de R\$ 793.199,04 (setecentos e noventa e três mil cento e noventa e nove reais e quatro centavos), conforme quadro demonstrativo abaixo:

Prestação de serviços técnicos de Administração e Operação Remota em Regime 24x7, com posto de trabalho no Ambiente de Tecnologia da Informação, em regime de 5 dias x 8 horas diárias (horário de expediente do CFC), a fim de gerenciamento do Ambiente de Tecnologia da Informação do Conselho Federal de Contabilidade (CFC).							
GRUPO	ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QTDE.	VALORES		
					VALOR UNITÁRIO	VALOR MENSAL	VALOR ANUAL (12 MESES)
01	01	Serviço de Suporte Técnico com Monitoramento de ativos 24x7 e Operação Remota (Centro de Operação Remoto)	Serviço	01	R\$ 14.537,50	R\$ 14.537,50	R\$ 174.450,00
	02	Analista de TI para a prestação de serviços técnicos de Administração, Suporte e Operação de Rede de Dados Local	Posto de Serviço	02	R\$ 25.781,21	R\$ 51.562,42	R\$ 618.749,04
VALOR TOTAL DO CONTRATO R\$ 793.199,04							

3.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

3.3. O valor acima é meramente estimativo, de forma que os pagamentos devidos à CONTRATADA dependerão dos quantitativos de serviços efetivamente prestados.

4. CLÁUSULA QUARTA – DOTAÇÃO ORÇAMENTÁRIA

4.1. As despesas para atender a esta licitação estão programadas em dotação orçamentária própria, Descrição da Conta: conta contábil 6.3.1.3.02.01.005 (Serviços de Tecnologia da Informação), de acordo com Orçamento Anual do CFC aprovado pela Resolução CFC nº. 1.609/2020.

4.2. No(s) exercício(s) seguinte(s), as despesas correspondentes correrão à conta dos recursos próprios para atender às despesas da mesma natureza, cuja alocação será feita no início de cada exercício financeiro.

5. CLÁUSULA QUINTA – PAGAMENTO

5.1. O prazo para pagamento à CONTRATADA e demais condições a ele referentes encontram-se definidos no Termo de Referência e no Anexo XI da IN SEGES/MP n. 5/2017.

6. CLÁUSULA SEXTA – REAJUSTAMENTO DE PREÇOS EM SENTIDO AMPLO.

6.1. As regras acerca do reajustamento de preços em sentido amplo do valor contratual (reajuste em sentido estrito e/ou repactuação) são as estabelecidas no Termo de Referência, anexo deste Contrato.

7. CLÁUSULA SÉTIMA – GARANTIA DE EXECUÇÃO

7.1. Será exigida a prestação de garantia na presente contratação, conforme regras constantes do Termo de Referência, anexo do Edital.

8. CLÁUSULA OITAVA – MODELO DE EXECUÇÃO DOS SERVIÇOS E FISCALIZAÇÃO

8.1. O modelo de execução dos serviços a serem executados pela CONTRATADA, os materiais que serão empregados, a disciplina do recebimento do objeto e a fiscalização pela CONTRATANTE são aqueles previstos no Termo de Referência, anexo do Edital.

9. CLÁUSULA NONA – OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

9.1. As obrigações da CONTRATANTE e da CONTRATADA são aquelas previstas no Termo de Referência, anexo do Edital.

10. CLÁUSULA DÉCIMA – SANÇÕES ADMINISTRATIVAS.

10.1. As sanções relacionadas à execução do contrato são aquelas previstas no Termo de Referência, anexo do Edital.

11. CLÁUSULA DÉCIMA PRIMEIRA – RESCISÃO

11.1. O presente Termo de Contrato poderá ser rescindido:

11.1.1. por ato unilateral e escrito da Administração, nas situações previstas nos incisos I a XII e XVII do art. 78 da Lei nº 8.666, de 1993, e com as consequências indicadas no art. 80 da mesma Lei, sem prejuízo da aplicação das sanções previstas no Termo de Referência, anexo ao Edital;

11.1.2. amigavelmente, nos termos do art. 79, inciso II, da Lei nº 8.666, de 1993.

11.2. Os casos de rescisão contratual serão formalmente motivados e precedidos de autorização da autoridade competente, assegurando-se à CONTRATADA o direito ao contraditório, bem como à prévia e ampla defesa.

11.3. A CONTRATADA reconhece os direitos da CONTRATANTE em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de 1993.

11.4. O termo de rescisão, sempre que possível, será precedido:

11.4.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

11.4.2. Relação dos pagamentos já efetuados e ainda devidos;

11.4.3. Indenizações e multas.

11.5. O não pagamento dos salários e das verbas trabalhistas, e o não recolhimento das contribuições sociais, previdenciárias e para com o FGTS poderá dar ensejo à rescisão do contrato por ato unilateral e

escrito do CONTRATANTE e à aplicação das penalidades cabíveis (art. 8º, inciso IV, do Decreto n.º 9.507, de 2018).

11.6. Quando da rescisão, o fiscal administrativo deverá verificar o pagamento pela CONTRATADA das verbas rescisórias ou os documentos que comprovem que os empregados serão realocados em outra atividade de prestação de serviços, sem que ocorra a interrupção do contrato de trabalho (art. 64 a 66 da IN SEGES/MP n.º 05/2017).

11.7. Até que a CONTRATADA comprove o disposto no item anterior, a CONTRATANTE reterá:

11.7.1. a garantia contratual, prestada com cobertura para os casos de descumprimento das obrigações de natureza trabalhista e previdenciária pela CONTRATADA, que será executada para reembolso dos prejuízos sofridos pela Administração, nos termos da legislação que rege a matéria; e

11.7.2. os valores das Notas fiscais ou Faturas correspondentes em valor proporcional ao inadimplemento, até que a situação seja regularizada.

11.8. Na hipótese do subitem anterior, não havendo quitação das obrigações por parte da CONTRATADA no prazo de quinze dias, a CONTRATANTE poderá efetuar o pagamento das obrigações diretamente aos empregados da CONTRATADA que tenham participado da execução dos serviços objeto do contrato.

11.9. O CONTRATANTE poderá ainda:

11.9.1. nos casos de obrigação de pagamento de multa pela CONTRATADA, reter a garantia prestada a ser executada, conforme legislação que rege a matéria; e

11.9.2. nos casos em que houver necessidade de ressarcimento de prejuízos causados à Administração, nos termos do inciso IV do art. 80 da Lei n.º 8.666, de 1993, reter os eventuais créditos existentes em favor da CONTRATADA decorrentes do contrato.

11.10. O contrato poderá ser rescindido no caso de se constatar a ocorrência da vedação estabelecida no art. 5º do Decreto n.º 9.507, de 2018.

12. CLÁUSULA DÉCIMA SEGUNDA – VEDAÇÕES

12.1. É vedado à CONTRATADA:

12.1.1. caucionar ou utilizar este Termo de Contrato para qualquer operação financeira;

12.1.2. interromper a execução dos serviços sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.

13. CLÁUSULA DÉCIMA TERCEIRA – ALTERAÇÕES

13.1. Eventuais alterações contratuais reger-se-ão pela disciplina do art. 65 da Lei nº 8.666, de 1993, bem como do ANEXO X da IN/SEGES/MP nº 05, de 2017.

13.2. A CONTRATADA é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

13.3. As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

14. CLÁUSULA DÉCIMA QUARTA – DOS CASOS OMISSOS

14.1. Os casos omissos serão decididos pela CONTRATANTE, segundo as disposições contidas na Lei nº 8.666, de 1993, na Lei nº 10.520, de 2002 e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

15. CLÁUSULA DÉCIMA QUINTA – PUBLICAÇÃO

15.1. Incumbirá à CONTRATANTE providenciar a publicação deste instrumento, por extrato, no Diário Oficial da União, no prazo previsto na Lei nº 8.666, de 1993.

16. CLÁUSULA DÉCIMA SEXTA – FORO

16.1. É eleito o Foro de Brasília para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não possam ser compostos pela conciliação, conforme art. 55, §2º, da Lei nº 8.666/93.

Para firmeza e validade do pactuado, o presente Termo de Contrato foi lavrado eletronicamente, que, depois de lido e achado em ordem, vai assinado pelos contraentes.

CONSELHO FEDERAL DE CONTABILIDADE

Carlos Rubens de Oliveira

Vice-Presidente Administrativo

Assinado via SEI

ISH TECNOLOGIA S/A

Vítor Teixeira Costa

Representante Legal

Assinado via SEI

Anexo I

DA INTEGRIDADE DOS CONTRATANTES

Este anexo contribui para materializar o compromisso das partes para o cumprimento do exposto nas Leis nº 12.846, de 01 de agosto de 2013, nº 13.709, de 14 de agosto de 2018, no Decreto nº 7.203, de 4 de junho de 2010, e na Norma Brasileira ABNT NBR ISO 37001, em relação à adequação a legislação pátria e boas práticas de governança, integridade e privacidade de dados.

O Conselho Federal de Contabilidade, por intermédio da Resolução CFC nº 1.563, de 14 de março de 2019, instituiu o Plano de Integridade, que define ações de promoção e fortalecimento das instâncias de integridade, por meio de mecanismos destinados à prevenção, à detecção, à punição e à remediação de fraudes e atos de corrupção.

As empresas licitantes deverão tomar conhecimento da Política Antifraude e Anticorrupção do CFC que poderá ser acessada em seu sítio eletrônico oficial e através do seguinte link: <https://cfc.org.br/programa-de-integridade/>

O CFC e a Contratada **concordam** que, durante a execução deste contrato, atuarão em conformidade com ordenamento jurídico brasileiro no que tange ao combate à corrupção e à fraude, e se comprometem a cumpri-los na realização de suas atividades, por seus executivos, sócios, diretores, coordenadores, representantes, administradores e colaboradores, assim como, **declara e garante que:**

Em relação ao Nepotismo:

1) seus atuais sócios, administradores, controladores ou dirigentes não ocupam cargo, emprego ou função no CFC ou em empresa prestadora de serviço no CFC;

2) seus atuais sócios, administradores, controladores ou dirigentes não possuem parentesco, até o terceiro grau, com qualquer ocupante de cargo, emprego ou função, mesmo que transitoriamente e sem remuneração, dentro de unidade administrativa do CFC que promova a licitação ou com ocupantes de cargo de direção, chefia ou assessoramento;

3) nos demais casos de parentesco, até o terceiro grau, de seus atuais sócios administradores, controladores, dirigentes com qualquer ocupante de cargo, emprego ou função no CFC, mesmo que transitoriamente e sem remuneração, declara que o parentesco não teve poder de influência na contratação;

4) que eventual ex-ocupante de cargo, emprego ou função do CFC que venha a integrar a Contratada, seja na qualidade de administrador, sócio, controlador ou dirigente, tenha rompido seu vínculo com o CFC há pelo menos 6 (seis) meses, obrigando-se a Contratada a informar por escrito, no prazo de 3 (três) dias úteis ao CFC qualquer nomeação de seus representantes em quaisquer das hipóteses elencadas.

Em relação às normas anticorrupção e antissuborno:

5) não realiza, não oferece; e não autoriza: qualquer pagamento ou promessa de pagamento como suborno; entrega de presente(s); concessão de entretenimento(s); fornecimento ou pagamento de refeição(ões), hospitalidade(s) ou qualquer outra vantagem direta ou indireta para o uso ou benefício de qualquer funcionário do CFC ou seus familiares; e não concede benefício direto ou indireto de partido político, de candidato a cargo eletivo, ou de qualquer outro indivíduo a qualquer funcionário do CFC ou seus familiares.

Em relação à proteção de dados pessoais:

6) para prestar os serviços relativos a esta contratação, deve se comprometer com a proteção dos Dados Pessoais de acordo com a Lei nº 13.709/2018 ("Lei Geral de Proteção de Dados Pessoais"), bem como quaisquer outras leis relativas à proteção de dados pessoais que vierem a ser promulgadas.

7) a Contratada deverá envidar esforços para proteção da informação, principalmente dos Dados Pessoais e Dados Pessoais Sensíveis – aplicando as medidas de proteção administrativa e técnica necessárias e disponíveis à época, caso haja dados pessoais que forem armazenados pelos sistemas de propriedade ou de utilização da Contratada.

8) durante a vigência do contrato, o titular dos Dados Pessoais tratados tem direito a obter da Contratada, a qualquer momento e mediante requisição, desde que em conformidade com normas legais e regulatórias:

I - confirmação da existência de tratamento de seus dados; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; VI - eliminação dos dados pessoais tratados com o consentimento do titular; VII - informação das entidades públicas e privadas com as quais se realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e IX - revogação do consentimento para o tratamento de dados.

O não cumprimento pela Contratada da legislação ou disposto neste Contrato, durante a execução deste, será considerado infração e conferirá ao CFC o direito de: instaurar procedimento de apuração de responsabilidade administrativa e rescindir o Contrato, após o devido processo legal, sendo a Contratada responsável por eventuais perdas e danos, nos termos da Lei Federal nº 12.846/ 2013 e do Decreto nº 8.420/2015, sem prejuízo da aplicação das sanções administrativas previstas nas leis 8.666/93 e 10.520/2002.



Documento assinado eletronicamente por **Carlos Rubens de Oliveira, Vice-Presidente**, em 02/11/2022, às 09:17, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Vitor teixeira Costa, Usuário Externo**, em 03/11/2022, às 09:48, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0057355** e o código CRC **6918F025**.

AVISO DE LICITAÇÃO
PREGÃO ELETRÔNICO Nº 67/2022 - UASG 90018

Nº Processo: 0004170-44.2022. Objeto: Contratação de serviços de engenharia para execução de impermeabilização de reservatório (cisterna) com argamassa polimérica e substituição de tubos, conexões e válvulas do sistema de prevenção a incêndio na sede da Subseção Judiciária de Curitiba. Total de Itens Licitados: 1. Edital: 09/11/2022 das 13h00 às 17h59. Endereço: Avenida Anita Garibaldi, 888 - 7º Andar, Cabral - Curitiba/PR ou <https://www.gov.br/compras/edital/90018-5-00067-2022>. Entrega das Propostas: a partir de 09/11/2022 às 13h00 no site www.gov.br/compras. Abertura das Propostas: 25/11/2022 às 14h00 no site www.gov.br/compras.

MARILEI BERBERT PADILHA
Supervisora do Setor de Processamento de Licitações

(SIASGnet - 08/11/2022) 90018-00001-2022NE000067

SEÇÃO JUDICIÁRIA DO RIO GRANDE DO SUL

EXTRATO DE INEXIGIBILIDADE DE LICITAÇÃO

PROCESSO: 0003202-20.2022.4.04.8001. OBJETO: contratação do evento Conferência Magna do Mês da Consciência Negra 2022, constituída de palestra online - 2h - conforme briefing de Alexandra Baldeh Loras, com o tema Diversidade Racial e Anti-racismo e de 3 (três) palestrantes para a Mesa-redonda e homenagem "O legado de Petronilha Beatriz Gonçalves e Silva para o antirracismo e a educação no Brasil", no dia 18 de novembro - 3h. CONTRATANTE: Justiça Federal de 1º Grau/RS. CONTRATADAS: Loras D&A Consultoria de Negócios Eventos e Conteúdo Audiovisual Ltda., CNPJ: 26.530.500/0001-29, no valor de R\$ 20.000,00 (vinte mil reais), Joana Celia dos Passos, CPF: 592.004.999-53, no valor de R\$ 824,99 (oitocentos e vinte e quatro reais e nove centavos), Fernanda Oliveira da Silva, CPF: 009.573.530-57, no valor de R\$ 824,99 (oitocentos e vinte e quatro reais e nove centavos) e Petronilha Beatriz Gonçalves e Silva, CPF: 009.148.430-87, no valor de R\$ 514,29 (quinhentos e quatorze reais e vinte e nove centavos). CRÉDITO ORÇAMENTÁRIO: PTRES 168360, NDZ: 33.90.39 e 33.90.36, NE: 2022NE000887, 2022NE000888, 2022NE000889 e 2022NE000890, de 03/11/2022. FUNDAMENTO LEGAL: artigo 25, inciso II, combinado com o art. 13, inciso VI, da Lei nº 8.666/93.

5ª REGIÃO

SEÇÃO JUDICIÁRIA DE ALAGOAS

EXTRATO DE TERMO ADITIVO

PA Nº 0000720-50.2022.4.05.7200. Primeiro Termo Aditivo do CONTRATO Nº 09/2022-JF/AL. PREGÃO ELETRÔNICO Nº 03/2022. CONTRATADA: NOBREGA & ASSIS SERVIÇOS DE ENGENHARIA LTDA. CNPJ: 24.995.315/0001-84. OBJETO: contratação de empresa especializada em serviços de engenharia para o fornecimento e instalação de sistema de microgeração de energia solar fotovoltaica on-grid no exercício sede da Seção Judiciária de Alagoas. FINALIDADE DO ADITIVO: prorrogação do prazo para execução do serviço mais 36 (trinta e seis) dias corridos, compreendendo o período de 06/11/2022 a 11/12/2022. FUNDAMENTO LEGAL: Art. 57, 1º parágrafo da Lei nº 8.666/93. DATA DA ASSINATURA: 08/11/2022. SIGNATÁRIOS: André Luís Maia Tobias Granja - Juiz Federal Diretor do Foro, pela Contratante; Beethoven Nobrega de Assis, Diretor Técnico, pela Contratada.

SEÇÃO JUDICIÁRIA NO RIO GRANDE DO NORTE

AVISO DE LICITAÇÃO
PREGÃO ELETRÔNICO Nº 21/2022 - UASG 90007

Nº Processo: SEI 2957-66.2022. Objeto: Renovação de Suporte e Garantia do Firewall. Total de Itens Licitados: 3. Edital: 09/11/2022 das 08h00 às 12h00 e das 13h00 às 17h59. Endereço: Rua Doutor Lauro Pinto, 245 - Candelária, - Natal/RN ou <https://www.gov.br/compras/edital/90007-5-00021-2022>. Entrega das Propostas: a partir de 09/11/2022 às 08h00 no site www.gov.br/compras. Abertura das Propostas: 23/11/2022 às 09h00 no site www.gov.br/compras. Informações Gerais: .

AMANDA CAVALCANTE OLIVEIRA
Supervisora da SLC

(SIASGnet - 08/11/2022) 90007-00001-2022NE000999

AVISO DE LICITAÇÃO
PREGÃO ELETRÔNICO Nº 20/2022 - UASG 90007

Nº Processo: SEI 2999-18.2022. Objeto: Serviço de engenharia para reestruturação da oficina e readequação da cobertura da Subseção Judiciária de Mossoró no Rio Grande do Norte (área total de 552,66 m²). Total de Itens Licitados: 1. Edital: 09/11/2022 das 08h00 às 12h00 e das 13h00 às 17h59. Endereço: Rua Doutor Lauro Pinto, 245 - Candelária, - Natal/RN ou <https://www.gov.br/compras/edital/90007-5-00020-2022>. Entrega das Propostas: a partir de 09/11/2022 às 08h00 no site www.gov.br/compras. Abertura das Propostas: 23/11/2022 às 09h00 no site www.gov.br/compras. Informações Gerais: .

AMANDA CAVALCANTE OLIVEIRA
Supervisora da SLC

(SIASGnet - 08/11/2022) 90007-00001-2022NE000999

DIRETORIA DO FORO

EXTRATO DE CONTRATO

CONTRATO Nº 25/2022-JF/RN. OBJETO: aquisição de notebooks e kit de produtividade com garantia de 60 (sessenta) meses para a JFRN. DELL COMPUTADORES DO BRASIL LTDA, CNPJ/MF nº 72.381.189/0010-01. PA 0003353-43.2022.4.05.7100-JFRN. PREGÃO 22/2022 - JFPE, ARP 14/2022-JFPE e Lei nº 10.520/2002. PTRES 168364, ED: 449052-41 - EQUIPAMENTOS DE TIC - COMPUTADORES. NE: 2022NE000361, de 28/10/2022. V. TOTAL: R\$ 130.419,75. VIGÊNCIA CONTRATUAL: 60 MESES a partir do recebimento definitivo. Assinado: em 07/11/2022, pela Contratante, Juiz Federal Carlos Wagner Dias Ferreira, Diretor do Foro e, em 04/11/2022, pela Contratada, Sr. Maurício Luís Cassalta de Paula Couto.

**Entidades de Fiscalização
do Exercício das Profissões Liberais**

CONSELHO FEDERAL DE CONTABILIDADE

EXTRATO DE INSTRUMENTO CONTRATUAL

Contrato nº 35/2022 - Processo SEI nº 90796110000007.000028/2022-91 - Pregão Eletrônico 11/2022. Contratante: Conselho Federal de Contabilidade; Contratada: ISH Tecnologia S/A. Objeto: gerenciamento do Ambiente de Tecnologia da Informação do Conselho Federal de Contabilidade (CFC) em Brasília - DF. Vigência: 03/11/2022 a 03/11/2023. Valor anual: R\$ 793.199,04 (setecentos e noventa e três mil, cento e noventa e nove reais e quatro centavos). Contratante: Carlos Rubens de Oliveira - Vice-Presidente Administrativo; Contratada: Vitor Teixeira Costa - Representante Legal.

AVISO DE SUSPENSÃO
PREGÃO Nº 20/2022

Comunicamos a suspensão da licitação supracitada, publicada no D.O.U em 31/10/2022. Objeto: Pregão Eletrônico - Aquisição de solução informatizada de privacidade, governança, riscos e compliance, na modalidade software como serviço (SaaS), contemplando apoio técnico para operação na adequação do CFC à Lei Geral de Proteção de Dados (LGPD), operação assistida, suporte e treinamento sobre as soluções (ferramentas) implantadas, a fim de atender às necessidades do Conselho Federal de Contabilidade.

ROBSON WEIDER MENDES DE ARAUJO
Pregoeiro

(SIDE - 08/11/2022) 383500-02022-2022NE000962

CONSELHO FEDERAL DE EDUCAÇÃO FÍSICA

RESULTADO DE LICITAÇÃO
PREGÃO ELETRÔNICO Nº 5/2022 - UASG 925042

Objeto: Contratação de empresa para prestação de serviços gráficos com fornecimento de materiais, objetivando a confecção personalizada de calendários de mesa e envelopes timbrados.

O Conselho Federal de Educação Física - CONFEF, por intermédio de seu Presidente, torna público o resultado do Pregão Eletrônico CONFEF nº 005/2022, conforme especificado abaixo:

Item 1 - Empresa: COAN INDUSTRIA GRÁFICA EIRELI, inscrita no CNPJ sob o nº 86.444.791/0001-64, no valor total de R\$ 212.812,00 (duzentos e doze mil e oitocentos e doze reais).

Item 2 - Empresa: SEIKE & MONTEIRO LTDA, inscrita no CNPJ sob o nº 11.184.290/0001-97, no valor total de R\$ 6.440,00 (seis mil, quatrocentos e quarenta reais).

CLAUDIO AUGUSTO BOSCHI
Presidente

CONSELHO FEDERAL DE ENGENHARIA E AGRONOMIA

EXTRATO DE CONTRATO

Contrato nº 219/2022, originário da Inexigibilidade de Licitação nº 208/2022, assinado em 4/11/2022; firmado com a SINALEIRO PROJETOS DE SINALIZAÇÃO VIÁRIA LTDA; Objeto: locação de estande para a participação do Confea na "AEA Convida: Gestão de Trânsito e Transporte", a ser realizada no período de 1º a 3/12/2022, em São Leopoldo - RS, Base legal: Lei nº 8.666/93, Vigência até o trigésimo dia subsequente ao do último dia fixado para realização do objeto patrocinado; Nota de Empenho nº 970/2022, Valor de R\$ 20.000,00 (vinte mil reais); Processo SEI Nº 00.004551/2022-66.

EXTRATO DE CONVÊNIO

Convênio nº 87/2022, assinado em 04/11/2022; firmado com o Crea-BA; Objeto: Auxílio financeiro ao programa Prodesu - PRODUFISC - II-A; Base legal: Lei nº 8.666/93, Decreto nº 6.170/07, Resolução nº 1.030/10, D. Normativas nº 087 e 088/11, P. Interministerial nº 424/2016 e Decisão PL nº 1481/2022; Vigência até 04/6/2023; Nota de Empenho nº 972 e 973/2022, Valor do Concedente: R\$ 323.683,70 e Conveniente: R\$ 101.528,41; Processo SEI Nº 00.001949/2022-41.

EXTRATO DE CONVÊNIO

Convênio nº 78/2022, assinado em 4/11/2022; firmado com o Crea-BA; Objeto: Auxílio financeiro ao programa Prodesu - II-D; Base legal: Lei nº 8.666/93, Decreto nº 6.170/07, Resolução nº 1.030/10, D. Normativas nº 087 e 088/11, P. Interministerial nº 424/2016 e Decisão PL nº 1379/2022; Vigência até 4/10/2023; Nota de Empenho nº 971/2022, Valor do Concedente: R\$ 439.466,07; Processo SEI Nº 00.003573/2022-17.

EXTRATO DE TERMO ADITIVO

2º Termo Aditivo ao Convênio nº 64/2019, firmado com o Crea-PI, assinado aos 28/10/2022; Objeto: alteração do Plano de Trabalho, cronograma, redução do valor total do convênio e prorrogação do prazo de vigência para 23/11/2023; Amparo: Lei nº 8666/93; Decreto nº 6170/07; Portaria Interministerial nº 424/2016 e Decisões Plenárias nºs 1125/2019 e 1516/2022; Processo SEI nº 04444/2019.

CONSELHO FEDERAL DE FISIOTERAPIA E TERAPIA OCUPACIONAL

AVISO DE ALTERAÇÃO
PREGÃO Nº 13/2022

Comunicamos que o edital da licitação supracitada, publicada no D.O.U de 18/10/2022 foi alterado. Objeto: Pregão Eletrônico - Contratação de empresa especializada na prestação de serviços de gerenciamento do abastecimento de combustíveis para a frota de veículos automotores do COFFITO. Total de Itens Licitados: 00001 Novo Edital: 09/11/2022 das 08h00 às 11h59 e de 12h00 às 17h59. Endereço: Srtvs Conj. I Lote 38701 Assis Chateaubriand Sala 602 BRASILIA - DF. Entrega das Propostas: a partir de 09/11/2022 às 08h00 no site www.comprasnet.gov.br. Abertura das Propostas: 22/11/2022, às 10h00 no site www.comprasnet.gov.br.

LUIZ FELIPE MATHIAS CANTARINO
Pregoeiro

(SIDE - 08/11/2022) 925168-00001-2022NE000001
(Of. El. nº .)

RESULTADO DE JULGAMENTO
PREGÃO ELETRÔNICO Nº 15/2022

O Conselho Federal de Fisioterapia e Terapia Ocupacional comunica o resultado do julgamento do Pregão Eletrônico (SRP) 15/2022. Objeto: Confecção de Cadernetas de Anotações Profissionais. Vencedora: EGF EDITORA GRÁFICA FATOR LTDA EPP, CNPJ 10.172.304/0001-90 - Valor Unitário - R\$11,65 (onze reais e sessenta e cinco centavos). Quantidade Registrada: 40.000 unidades.

LUIZ FELIPE MATHIAS CANTARINO
Pregoeiro



Este documento pode ser verificado no endereço eletrônico
<http://www.in.gov.br/autenticidade.html>, pelo código 05302022110900172





CONSELHO FEDERAL DE CONTABILIDADE
SAUS Quadra 05, Lote 03, Bloco J, Edifício CFC, - Bairro Asa Sul, Brasília/DF, CEP 70070-920
Telefone: +55 61-3314-9600 - E-mail: cfc@cfc.org.br - www.cfc.org.br

TERMO DE REFERÊNCIA

Processo nº 90796110000007.000028/2022-91

1. OBJETO

1.1. Contratação de empresa especializada para prestação de serviços técnicos de Administração e Operação em Regime 24x7, com posto de trabalho no Ambiente de Tecnologia da Informação, em regime de 5 dias x 8 horas diárias (horário de expediente do CFC) a fim de gerenciamento do Ambiente de Tecnologia da Informação do Conselho Federal de Contabilidade (CFC) em Brasília – DF, conforme especificação no Anexo I, deste Termo de Referência.

1.2. O objeto da licitação tem a natureza de serviço comum, de que tratam a Lei n.º 10.520/2002 e o Decreto n.º 10.024/2019, por possuir padrões de desempenho e características gerais e específicas, usualmente encontradas no mercado, podendo, portanto, ser licitado por meio da modalidade Pregão, na forma eletrônica, tendo como critério de julgamento o menor preço global.

1.3. A prestação do serviço não gera vínculo empregatício entre os empregados da Contratada e o CFC, vedando-se qualquer relação, entre estes, que caracterize pessoalidade e subordinação direta.

GRUPO	ITEM	CATMAT/CATSER	DESCRIÇÃO	QTDE.
01	01	27340	Serviço de Suporte Técnico com Monitoramento de ativos 24x7 e Operação Remota (Centro de Operação Remoto).	01
	02	27340	Analista de TI para a prestação de serviços técnicos de Administração, Suporte e Operação de Rede de Dados Local.	02

1.4. Os quantitativos e respectivos códigos dos itens são os discriminados na tabela acima e descrição dos serviços no Anexo I.

1.5. O prazo de vigência do contrato será pelo período de 12 (doze) meses, podendo ser renovado, quando for comprovadamente vantajoso para o CFC, por iguais e sucessivos períodos, até o limite de 60 (sessenta) meses, observados os requisitos do art. 57, II, da Lei n.º 8.666/93 c/c art. 15, Instrução Normativa n.º 5, de 26 de maio de 2017.

2. JUSTIFICATIVA PARA A CONTRATAÇÃO DA SOLUÇÃO E DO SERVIÇO

2.1. A execução dos serviços atenderá às necessidades do Conselho Federal de Contabilidade em relação às atividades desenvolvidas por especialista em administração de rede de dados, no qual o CFC não dispõe do cargo exigido em seu plano de cargos e salários. Devido a complexidade imposta pela heterogeneidade das ferramentas e da necessidade de especialização para a administração dos sistemas, este órgão considerada como ponto importante a contratação e manutenção de empresa especializada para auxiliar nas tarefas listadas como rotineiras, descritas neste termo de referência, além de auxiliar a equipe de Tecnologia da Informação do CFC nos projetos que seguirão.

2.2. Em decorrência da aplicação de novos recursos adotados pelo mercado, no que se refere à infraestrutura de Tecnologia da Informação, pretende-se realizar com esta contratação a adoção de novos procedimentos visando melhorar os processos do CFC por meio do ITIL e COBIT e NBR ISO-20000. Serão implementados, no decorrer da vigência do contrato, serviços, tais como: gerenciamento de nível de serviço, gerenciamento de incidentes, gerenciamento de configuração, gerenciamento de mudanças e gerenciamento de disponibilidade. Além disso, serão registradas informações sobre o andamento dos trabalhos e desenvolvidas ferramentas para administração da capacidade produtiva. Este sistema deverá comportar as especificidades das áreas de suporte a redes local e de longa distância, acompanhamento de contratos e segurança da informação.

2.3. A contratação, objeto deste Termo de Referência, busca alcançar os seguintes resultados: criar um nível de infraestrutura de rede de dados adequada e adaptada à dinâmica dos processos de negócios do CFC e a elaborar soluções para garantir a privacidade e segurança das informações do Conselho Federal de Contabilidade, visando assegurar a continuidade das suas atividades institucionais.

2.4. Cabe destacar que o ambiente informatizado do CFC está estável, com processo de produção em definição. Porém, carece de formalização e aplicação de boas práticas de governança para ambientes de infraestrutura de TI. Os serviços disponibilizados foram concebidos para atender de maneira singular a cada grupo de usuários e seus objetivos institucionais.

2.5. Aplicações como os sistemas publicados na Internet, o correio eletrônico, o site institucional do Conselho Federal de Contabilidade e os bancos de dados que suportam as aplicações existentes no ambiente de TI, sendo estes precedidos por níveis de SLA altíssimos e são aplicações críticas para este Conselho e consequentemente, pessoal técnico especializado deveria estar disponível também em período integral (24x7) para garantir os novos níveis de disponibilidade exigidos, o que não ocorre atualmente e seria financeiramente inviável implantar com o reduzido corpo técnico deste Conselho.

2.6. A prestação de serviços atual não acompanhou as necessidades e demandas das áreas de negócio do CFC, de forma que esse processo ficou aquém da realidade para atender aos diversos serviços de TI. Assim sendo, a contratação dos serviços ora especificados, são vitais para o cumprimento dos objetivos institucionais do Conselho Federal de Contabilidade.

2.7. Devido a abrangência de atuação do CFC, um grande risco para as atividades desenvolvidas é tornar os sistemas computacionais indisponíveis e colocá-los em risco a confidencialidade e a integridade dos dados nele armazenados. Além disso, ao ser comprometido, a infraestrutura de TI provida pode acarretar dano direto aos serviços disponibilizados aos cidadãos, gerando elevados transtornos ou ineficiência dos serviços públicos. É de grande importância que a infraestrutura de TI do CFC possua um monitoramento 24x7 consistente através de um Centro de Operação de Rede (NOC), provido através de um ambiente seguro, regido por normas de segurança da informação.

2.8. Portanto, em decorrência dos fatos ora expostos, o Conselho Federal de Contabilidade não dispõe de funcionários para atender à demanda dessas atividades, notadamente, na prestação de serviços de suporte e administração de rede de dados local, rede de dados de longa distância, rede de dados local nos Estados e de segurança da informação, bem como infraestrutura de Datacenter para manter serviços publicados para internet com elevado nível de segurança dos dados e disponibilidade das informações.

2.9. Os serviços que serão prestados pelos analistas de rede viabilizarão monitoramento do ambiente de TI, e atenderão as atividades (acessórias para as quais inexistem a previsão de cargos específicos no Plano de Cargos e Salários do CFC, tornando imprescindível a terceirização pretendida, com regime de dedicação exclusiva de mão de obra.

2.10. A Portaria MPDG n.º 443, de 27 de dezembro de 2018, estabelece os serviços que são preferencialmente objeto de execução indireta mediante contratação de serviços terceirizados. O normativo regulamenta o Art. 2º do Decreto n.º 9.507/2018 e elenca uma lista de serviços que podem ser terceirizados, sempre de caráter auxiliar, instrumental ou acessório, entre eles, estão os profissionais objetos da pretensa contratação.

2.11. Tal dispositivo retrata, mais uma vez, que as atribuições dos empregados do CFC devem ser voltadas ao planejamento, supervisão, orientação, coordenação e desenvolvimento de atividades relacionadas à fiscalização (poder de polícia), normatização, registro, educação continuada ou estratégias ou, ainda, atividades que envolvam a tomada de decisão ou posicionamento institucional em quaisquer áreas (planejamento, coordenação, supervisão e controle).

2.12. A finalidade das tarefas que serão desempenhadas pelos analistas de rede é garantir a operacionalização integral das aplicações finalísticas (atreladas à fiscalização, registro, normatização e educação continuada) por meio da ação de monitoramento do ambiente de Tecnologia de Informação do CFC. Para atingir esse objetivo o CFC vem buscando, de forma racional e persistente, obter melhor emprego de seus escassos recursos visando atingir a eficácia e eficiência de suas ações. Essa difícil missão, muitas vezes, torna-se impossível de ser cumprida a contento, em razão da falta de uma estrutura específica para execução de tarefas que, embora sejam consideradas auxiliares, são imprescindíveis para o funcionamento das organizações, como é o caso dos serviços terceirizados que se pretende licitar.

2.13. Buscando sempre a prática dos princípios da eficiência e efetividade, quando se tenta alcançar a alta produtividade, agilidade, qualidade, segurança e máxima perfeição do trabalho, as adequações dos atuais serviços são as metas visadas pelo CFC das atividades de analista de rede, o que não seria possível sem a contratação de serviços especializados terceirizados.

2.14. Em suma, os serviços pretendidos estão relacionados às atividade-meio e acessórias como definido no Decreto n.º 9.507/2017. Portanto, torna-se essencial a contratação frente às demandas na execução de atividades que não tenham relação com a missão institucional do CFC.

2.15. A presente contratação enquadra-se na categoria de serviços comuns, posto que todas as atividades a serem desenvolvidas serão executadas por profissional cuja categoria é reconhecida legalmente e está relacionada na Classificação Brasileira de Ocupações – CBO, disponível, a qualquer tempo, em um mercado próprio e estável composto por diversas empresas prestadoras desses serviços, as quais são comparáveis entre si, de modo que permite que a licitação seja realização por Pregão, na modalidade eletrônica.

2.16. O alinhamento ao planejamento estratégico do Sistema CFC/CRCs, Objetivo Estratégico 8 - Garantir a qualidade e confiabilidade nos processos e nos procedimentos e, ao Plano Diretor de Tecnologia da Informação (PDTI) do CFC 2020/2021, Diretriz 4 - Garantir que o acesso, o tratamento e o armazenamento de informações do Conselho Federal de Contabilidade ocorram em conformidade com políticas e normas que assegurem a confidencialidade e a integridade das informações.

2.17. No cenário atual do CFC, é crescente a demanda pela disponibilização online de serviços com alta disponibilidade, confiabilidade e tolerância a falhas. Nesse ambiente de missão crítica são necessários mecanismos que melhorem a eficiência dessa infraestrutura, reduzindo custos e simplificando o gerenciamento destes ativos. Estes mecanismos aprimoram a operação da infraestrutura, reduzindo o tempo de interrupção e consequentemente melhorando os níveis de serviço.

2.18. É importante frisar que, tão importante quanto efetuar a presente contratação, é garantir que a mesma atenda aos melhores critérios técnicos sinalizados pelo mercado de Tecnologia da Informação, respeitando os princípios da economicidade, eficiência e eficácia de grande relevância para as ações governamentais, ao mesmo tempo que subsidia a disponibilidade dos serviços de TI.

2.19. O acesso aos sistemas, rede de dados, é considerado ambiente de missão crítica, pois pode provocar a indisponibilidade de serviços importantes oferecidos aos empregados do CFC, aos Conselhos Regionais de Contabilidade, aos profissionais da contabilidade e à sociedade. Desta forma existe a indicação de uso de dois links para funcionarem com redundância, aumentando, assim, a resiliência da solução como um todo.

2.20. Espera-se que esta implantação possa elevar o nível de serviço prestado pelo CFC aos Conselhos Regionais de Contabilidade, aos profissionais da contabilidade e à sociedade, com confiabilidade e segurança.

3. DESCRIÇÃO DA SOLUÇÃO

3.1. A descrição dos serviços técnicos, objeto deste Termo de Referência, estão discriminados no Anexo I.

4. ESPECIFICAÇÕES DOS REQUISITOS DA CONTRATAÇÃO

4.1. Parque de informática da Contratante

4.1.1. No objeto da contratação estão compreendidas as atividades serviços técnicos de Administração e Operação Remota em Regime 24x7, com posto de trabalho no Ambiente de Tecnologia da Informação, em regime de 5 dias x 8 horas diárias (horário de expediente do CFC), tendo como base as seguintes características do parque de informática do CFC, conforme discriminado na tabela do subitem 4.1.3.

4.1.2. O ambiente tecnológico atual do Conselho Federal de Contabilidade se encontra atualizado com o uso de tecnologias recentes como virtualização, solução de armazenamento storage com deduplicação, e componentes de segurança (ex.: firewalls) recentemente renovados.

4.1.3. Compõem o ambiente tecnológico do Conselho Federal de Contabilidade os seguintes ativos:

TIPO	DESCRIÇÃO	QUANTIDADE
Appliance	Firewall – ForcePoint	02
Appliance	Blade - Huawei 08 LAMINAS REDE FC	01
Appliance	Storage – NetApp FAS 2240-2 REDE ISCI	01
Appliance	Storage – Huawei Dorado	01
Appliance	Mcafee Web Gateway	01
Appliance Virtual	Kaspersky Antispam	01
Appliance Virtual	kaspersky Endpoint	01
Hypervisor	Hyper-V	08
Hypervisor	Vmware ESXi 6.0	02
Servidor	Servidor com S.O. Linux	15
Servidor	Servidor com S.O. Windows	40
Estação	Estação de Trabalho	278
Notebook	Notebook ou Netbook	240
Switch	Switch LAN	21
Switch	Switch CORE	4
AP	Aruba IAP-103	40

4.2. Os serviços, detalhados no Anexo I deste Termo de Referência, possuem como propósito monitorar, administrar, gerenciar e operar a Rede de dados local – LAN, WAN, Rede de dados VPN entre os estados, Sistemas operacionais, Ambiente de Produção, Bancos de Dados através de um Centro Remoto 24x7, com posto de trabalho no Ambiente de Tecnologia da Informação, de acordo com as melhores práticas de segurança da informação, que integram o Sistema CFC/CRCs e estrutura do Conselho Federal de Contabilidade, de modo a assegurar a disponibilidade dos serviços de conectividade dessas Redes dentro dos parâmetros estabelecidos pelo CFC.

4.3. Prover um serviço especializado de infraestrutura remota para publicação do portal CFC, de acordo com melhores práticas de segurança da informação, mantendo a integridade, confidencialidade, autenticidade e disponibilidade dos dados.

4.4. Os serviços de segurança compreendem, dentre outros: elaboração / atualização / mensuração da arquitetura de segurança estabelecida pelo Conselho; resposta / prevenção de incidentes de segurança da informação; monitoração / informação do ambiente mencionado na tabela de ativos.

5. EXECUÇÃO DO OBJETO

5.1. Os serviços deverão ser implantados no CFC, localizado à SAUS, Quadra 5, Bloco J, Lote 3, Brasília/DF, em até 10 (dez) dias corridos a partir da data da assinatura do contrato e compreendem:

GRUPO	ITEM OU SERVIÇO	LOCAL DE EXECUÇÃO	HORÁRIO	PERÍODO	CARGA HORÁRIA
01	01	Serviço de Suporte Técnico com Monitoramento de ativos 24x7 e Operação Remota (Centro de Operação Remoto) Competências técnica item 5 do anexo I Especificações item 6 e 7 do anexo I	Serviço de Suporte e monitoramento de ativos: 24 x 7 Serviço de Operação Remoto: 16 x 5 dias úteis (fora do horário de expediente) e 24 x 2 dias não úteis)	Segunda à Domingo	Suporte e monitoramento: 168 horas Operação Remota 128 horas semanais
	02	Analista de TI para a prestação de serviços técnicos de Administração, Suporte e Operação de Rede de Dados Local Competências técnica item 4 do anexo I Especificações item 7 do anexo I	8 x 5 dias úteis (Segunda à Sexta) Horário de expediente do CFC	Segunda à Sexta	40 horas semanais

5.2. Para a execução dos serviços, a Contratada, além da Administração e Operação Remota conforme horários especificados,

deverá disponibilizar 02 (dois) profissionais para posto de trabalho na sede do CFC, pertencente à seguinte categoria de ocupação, conforme a Classificação Brasileira de Ocupações (CBO):

ATIVIDADE OU SERVIÇO	HORÁRIO	PERÍODO	CÓDIGO	OCUPAÇÃO
Serviços técnicos de suporte e Administração, suporte e operação de Rede de Dados Local	08 horas (horário de expediente do CFC)	Segunda a Sexta	2124-10	Analista de redes e de comunicação de dados

5.3. Os serviços serão executados pelos profissionais, conforme horário de trabalho estabelecido na tabela abaixo:

Profissional da Equipe Horário de Trabalho	
Serviço de Suporte Técnico com Monitoramento de ativos 24x7 e Operação Remota	Serviço de Suporte e monitoramento de ativos: 24 x 7 Serviço de Operação Remoto: 16 x 5 dias úteis (fora do horário de expediente) e 24 x 2 dias não úteis
Serviços técnicos de suporte e Administração de Rede de Dados Local	8 x 5 dias úteis Horário de expediente do CFC

5.4. Jornada de trabalho.

5.4.1. Os serviços técnicos de suporte e administração de rede de dados local deverão ser prestados de acordo com o disposto neste Termo de Referência, podendo haver flexibilidade, admitindo-se a compensação para o cumprimento de segunda à sexta-feira, desde que atendidas as normas trabalhistas vigentes.

5.4.2. Não há previsão para pagamento de horas extras para os postos de serviço.

5.4.3. Os serviços deverão ser executados de segunda à sexta-feira, das 8h às 17h30, observados os intervalos legais para alimentação.

5.4.4. Excepcionalmente, os serviços poderão ser realizados em dias e horários extraordinários, previamente autorizados por escrito pelo gestor do contrato do CFC.

5.4.4.1. Os serviços a que se referem o subitem anterior são aqueles que necessitem da presença física dos trabalhadores da contratada, após evidenciada a impossibilidade de resolução do chamado ou do atendimento da demanda pelo serviço remoto.

5.4.5. Não serão concedidos aos trabalhadores da contratada direitos típicos dos empregados do CFC, tais como recesso, ponto facultativo, dentre outros, exceto mediante as hipóteses de compensação de jornada previamente convencionadas e/ou autorizadas, a critério e no interesse da administração.

5.4.6. Nas hipóteses de faltas aos serviços em decorrência de paralização do transporte público, interesses particulares e quaisquer situações semelhantes, não havendo a imediata cobertura do posto de trabalho, o CFC fica autorizado a processar a glosa proporcional ou total das horas não trabalhadas, ficando, todas as obrigações trabalhistas decorrentes das referidas faltas, integralmente sob responsabilidade da Contratada.

5.4.7. A Contratada deverá efetuar o controle diário da jornada de trabalho dos empregados e apresentar ao CFC sempre que solicitado pelo fiscal do contrato. Esse controle poderá ser por registro manual, mecânico ou eletrônico, conforme estabelece o Art. 74 § 2º da CLT. Caso a contratada decida realizar o controle da jornada por meio mecânico ou eletrônico, o equipamento deverá ser fornecido e instalado, pela contratada, na sede do CFC, em até 15 (quinze) dias úteis da data de assinatura do contrato. No caso de instalação de Registrador Eletrônico de Ponto (REP), este deverá atender às regras constantes na Portaria n.º 1.510/2009 – MTE.

5.4.7.1. Os funcionários da Contratada deverão registrar o ponto nos horários de início e término de sua jornada de trabalho, bem como nos horários de repouso para refeição.

5.4.7.2. O CFC poderá alterar, durante a execução do contrato, o horário de início e término do posto de trabalho para melhor dimensionamento das atividades a serem executadas, sem prejuízo do cumprimento da jornada de trabalho.

5.4.7.3. A empresa Contratada deverá assegurar a disponibilização diária e integral dos postos com dedicação exclusiva de mão de obra, sem que ocorram faltas ou atrasos sem cobertura.

5.4.8. A Contratante deverá apresentar, mensalmente, ao fiscal do contrato o registro da frequência dos empregados (inclusive no caso de cobertura) e sempre que solicitado.

5.5. Crachás de Identificação

5.5.1. A Contratada deverá fornecer crachás de identificação aos empregados, no prazo máximo de 5 (cinco) dias úteis, a contar do início da prestação dos serviços, e, posteriormente, todos os empregados da empresa alocados no CFC deverão, obrigatoriamente, portar sua identificação.

5.5.2. A Contratada obriga-se a manter seus empregados, quando nas dependências do CFC, devidamente identificados mediante uso constante de crachá, que deverá ser fornecido sem qualquer ônus adicional ao CFC.

5.5.3. O crachá de identificação deverá conter fotografia recente, nome do empregado, número do RG, função do empregado bem como o nome e o logotipo da Contratada.

6. MODELO DE GESTÃO DO CONTRATO E CRITÉRIOS DE MEDIÇÃO

6.1. A gestão do contrato consiste no gerenciamento das atividades de fiscalização e gestão da execução contratual, visando

garantir o cumprimento das cláusulas contratuais avençadas e a solução de quaisquer problemas relativos ao objeto da contratação.

6.2. Participam da gestão do contrato os funcionários do CFC, que serão designados por meio de Portaria específica, onde constará suas atribuições e responsabilidades:

6.2.1. Gestor do contrato: responsável por coordenar toda a execução do contrato, desde as atividades relacionadas à fiscalização técnica até ao acompanhamento da documentação pertinente para formalização dos procedimentos de pagamento, prorrogação, eventual aplicação de sanções, dentre outros, conforme estabelecido no inciso I, do art. 40 da IN SEGES 5/2017.

6.2.2. Fiscal Técnico: responsável pelo acompanhamento da execução do objeto do contrato, aferindo se a prestação dos serviços está compatível com o exigido em ato convocatório para fins de pagamento, conforme estabelecido no inciso II, do art. 40 da IN SEGES 5/2017.

6.2.3. Fiscal Administrativo: responsável pelo acompanhamento dos aspectos administrativos da execução dos serviços, tais como as obrigações previdenciárias, fiscais e trabalhistas, além de tomar as providências tempestivas no caso de inadimplemento, conforme estabelecido no inciso III do art. 40 da IN SEGES 5/2017.

6.3. A execução dos serviços a serem executados terá acompanhamento dos empregados indicados pelo CFC, para atuarem como gestores e fiscais do contrato, os quais deverão observar a obrigatoriedade de elaborar, mensalmente, relatório de acompanhamento constando a medição, a avaliação do desempenho da Contratada e as possíveis ocorrências relativas ao descumprimento de cláusulas contratuais, subsidiando o aceite, o ateste e a efetivação do pagamento em conformidade com a Instrução Normativa MPDG nº 05/2017 e suas alterações.

6.4. A Contratada deverá manter o preposto como meio principal de comunicação entre a prestadora de serviços e o CFC, que designará os fiscais administrativo, técnico e o Gestor do Contrato.

6.5. Em observância ao disposto no § 2º, art. 44 da IN SEGES 5/2017, a comunicação entre o CFC e a contratada “deve ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se, excepcionalmente, o uso de mensagem eletrônica para esse fim.” A comunicação oficial entre o CFC e a Contratada se dará por intermédio do preposto e por meio de documentação escrita (ofício, circulares ou correio eletrônico institucional).

6.6. Deverão ocorrer reuniões periódicas para alinhamento dos serviços a serem prestados e debate acerca da qualidade dos serviços. Todos os entendimentos das reuniões deverão constar da ata de reunião a ser lavrada pelo fiscal do contrato e assinada por todos os participantes.

6.7. Durante a vigência do contrato o CFC adotará o Instrumento de Medição de Resultado (IMR) - Anexo II - de acordo com os parâmetros estabelecidos na IN SEGES/MPDG n.º 05/2017.

6.7.1. O IMR é o mecanismo que define, em bases compreensíveis, tangíveis, objetivamente observáveis e comprováveis, os níveis esperados de qualidade da prestação do serviço e respectivas adequações de pagamento;

6.7.2. A forma de medição do serviço e pagamento à Contratada será por Acordo de Níveis de Serviços. Os indicadores mínimos de desempenho para aferição da qualidade esperada da prestação dos serviços constam do Anexo II deste Termo de Referência.

6.7.3. Mensalmente, a fiscalização do contrato deverá verificar o nível de atendimento aos indicadores previstos no IMR.

6.8. O pagamento aos profissionais dos postos de serviço se dará pela plena execução dos serviços, de acordo com o regime de cada cargo e a partir da data de início da prestação dos serviços conforme previsão contratual.

6.9. Em caso de não cumprimento das metas estabelecidas, o fiscal efetuará as glosas na medição dos serviços, conforme demonstrativo Anexo II e o entregará à Contratada para emissão da Nota Fiscal, com os devidos descontos.

7. INFORMAÇÕES RELEVANTES PARA O DIMENSIONAMENTO DA PROPOSTA

7.1. A demanda do órgão tem como base as seguintes características:

7.1.1. Os serviços serão executados na sede do Conselho Federal de Contabilidade, localizado no SAUS, Quadra 05, Bloco J, Edício CFC em Brasília/DF.

7.1.2. O cálculo dos salários dos empregados deverá basear-se em Convenção Coletiva de Trabalho da categoria vigente à data do Pregão Eletrônico, conforme estipulado no item 5.2 deste Termo de Referência.

7.1.3. Os horários da prestação de serviços por todos os profissionais obedecerão o item 5.4 deste Termo de Referência.

7.1.4. Os valores da proposta, incluindo todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na prestação dos serviços, deverão ser apurados pela licitante mediante o preenchimento do modelo de Planilha de Custos e Formação de Preços.

7.1.5. É vedado à proponente incluir na Planilha de Custos e Formação de Preços:

a) Item relativo a despesas decorrentes de disposições contidas em Acordos, Convenções ou Dissídios Coletivos de Trabalho que tratem de pagamento de participação dos trabalhadores nos lucros ou resultados da empresa contratada, de matéria não trabalhista, ou que estabeleçam direitos não previstos em lei, tais como valores ou índices obrigatórios de encargos sociais ou previdenciários, bem como de preços para os insumos relacionados ao exercício da atividade (art. 9º, parágrafo único, incisos I a III, do Decreto n.º 9.507/2018, e art. 6º da IN SEGES/MP n.º 5, de 2017);

b) Item relativo a despesas decorrentes de disposições contidas em Acordos, Convenções ou Dissídios Coletivos de Trabalho que tratem de obrigações e direitos que somente se aplicam aos contratos com a Administração Pública (art. 6º, parágrafo único, da IN SEGES/MP n.º 5/2017);

c) Rubricas que prevejam o custeio de despesas com treinamento, reciclagem e capacitação ou congêneres, pois tais parcelas já são cobertas pelas despesas administrativas (Acórdão TCU nº 2.746/2015 - Plenário);

d) Rubrica denominada “reserva técnica”, exceto se houver justificativa, na proposta, que indique, claramente e por meio de memória de cálculo, o que está sendo custeado, de modo a haver a comprovação da não cobertura do valor, direta ou indiretamente, por outra rubrica da planilha (Acórdãos TCU nº 2.746/2015 – Plenário, nº 64/2010 - 2ª Câmara e nº 953/2016 - Plenário);

e) Rubrica para pagamento do Imposto de Renda Pessoa Jurídica - IRPJ e da Contribuição Social Sobre o Lucro Líquido – CSLL (Súmula TCU nº 254/2010);

f) Rubrica denominada “verba” ou “verba provisional”, pois o item não está vinculado a qualquer contraprestação mensurável (Acórdãos TCU nº 1.949/2007 – Plenário e nº 6.439/2011 – 1ª Câmara);

7.1.6. A licitante deverá apresentar a proposta conforme modelo Anexo V deste Termo de Referência.

7.1.7. A apresentação da proposta implicará plena aceitação, por parte da proponente, das condições estabelecidas neste Termo de Referência e em Edital.

7.1.8. Sindicatos da Categoria - A contratada está obrigada a observar, tanto na formulação da proposta quanto na execução contratual, as exigências constantes de Acordos Coletivos de Trabalho que alcançam as categorias pertinentes à prestação dos serviços.

7.1.9. Na elaboração da planilha de formação de preços, o licitante poderá utilizar norma coletiva de trabalho diversa daquela adotada pelo CFC como parâmetro para o orçamento estimado da contratação, tendo em vista que o enquadramento sindical do empregador é definido por sua atividade econômica preponderante, e não em função da atividade desenvolvida pela categoria profissional que prestará os serviços mediante cessão de mão de obra, conforme disciplina o Acórdão TCU nº 1097/2019-Plenário:

a) a desclassificação da empresa RCS Tecnologia, em razão da CCT utilizada em sua proposta, ocorreu de forma indevida, tendo em vista que os valores estabelecidos estão em conformidade com o previsto em Convenção Coletiva de Trabalho relacionada à atividade principal da empresa licitante, em atenção aos artigos 570, 577 e 581, § 2º da CLT e à luz da Constituição Federal (art. 8º, inciso II), bem como Acórdão 859/2016-TCU-Plenário, Relator Ministro Augusto Nardes.

[...]

9.3.1. utilização na planilha de formação de preços de norma coletiva do trabalho diversa da utilizada pela Agência para a elaboração do orçamento estimado da contratação, tendo em vista que o enquadramento sindical é aquele relacionado à atividade principal da empresa licitante e não da categoria profissional a ser contratada, em atenção aos artigos 570, 577 e 581, § 2º da CLT e ao art. 8º, II, da Constituição Federal.

7.1.10. Será exigida a garantia de execução do contrato, nos moldes do art. 56 da Lei nº 8.666, de 1993, conforme estabelecido no item 23 deste Termo de Referência.

7.1.11. A empresa contratada deverá cumprir os prazos, abaixo, além de outros estabelecidos neste Termo de Referência:

DESCRIÇÃO	PRAZO
Duração do contrato	12 (doze) meses após assinatura do contrato
Autorizar o CFC a fazer o desconto nas faturas e realizar os pagamentos dos salários e demais verbas trabalhistas diretamente aos trabalhadores, bem como das contribuições previdenciárias e do FGTS, quando não demonstrado o cumprimento tempestivo e regular dessas obrigações, até o momento da regularização, sem prejuízo das sanções cabíveis.	No ato da assinatura do contrato.
Início da prestação de serviços.	Até 10 (dez) dias úteis após a assinatura do contrato.
Fornecimento e instalação do Registrador Eletrônico de Ponto (em caso de opção pelo controle da jornada por meio mecânico ou eletrônico).	Até 15 (quinze) dias úteis após início após a assinatura do contrato.
Fornecer crachá de identificação para os empregados.	Até 5 (cinco) dias úteis após início da prestação de serviços
Orientar os empregados sobre o Plano de Logística Sustentável (PLS) e Normas Internas e de Segurança e Medicina no Trabalho do CFC	Até 30 (trinta) dias úteis após o início da prestação de serviços
Apresentar ao CFC os documentos listados no item 9.4 do TR	Primeiro mês da prestação dos serviços.
Apresentar ao CFC os documentos listados no item 9.4 do TR	Imediatamente após a contratação de novo empregado
Apresentar relação mensal dos empregados que optarem por não receber vale transporte (subitem 9.5 do TR)	Mensalmente.
Substituir empregado em caso de eventual ausência e comunicar ao CFC	Em até 3 (três) horas da ausência.

Viabilizar o acesso de seus empregados, via internet, por meio de senha própria, aos sistemas da Previdência Social e da Receita Federal do Brasil, com o objetivo de verificar se as suas contribuições previdenciárias foram recolhidas.	Até 60 (sessenta) dias contados do início da prestação dos serviços ou da admissão do empregado.
Viabilizar a emissão do cartão cidadão pela Caixa Econômica Federal para todos os empregados	Até 60 (sessenta) dias contados do início da prestação dos serviços ou da admissão do empregado.
Apresentar cópia do ofício enviado à Receita Federal do Brasil, com comprovante de entrega e recebimento, comunicando a assinatura do contrato de prestação de serviços mediante cessão de mão de obra.	Até o último dia do mês subsequente ao da ocorrência da situação de vedação.
Comunicar ao Fiscal do contrato qualquer ocorrência anormal ou acidente que se verifique no local dos serviços.	Até 24 (vinte e quatro) horas da ocorrência.
Substituir empregado cuja atuação, permanência e/ou comportamento sejam julgados prejudiciais, inconvenientes e/ou insatisfatórios	Até 24 (vinte e quatro) horas da notificação.
Comunicar o CFC sempre que ocorrer desligamento de empregado	Até 24 (vinte e quatro) horas do ocorrido.
Substituir empregado desligado/demitido	Até 24 (vinte e quatro) horas do ocorrido.
Apresentar a seguinte documentação: a.1. relação dos empregados, contendo nome completo, cargo ou função, horário do posto de trabalho, números da carteira de identidade (RG) e da inscrição no Cadastro de Pessoas Físicas (CPF), com indicação dos responsáveis técnicos pela execução dos serviços, quando for o caso; a.2. Carteira de Trabalho e Previdência Social (CTPS) dos empregados admitidos e dos responsáveis técnicos pela execução dos serviços, quando for o caso, devidamente assinada pela contratada; e a.3. exames médicos admissionais dos empregados da contratada que prestarão os serviços. c) entregar, quando solicitado pelo CFC, de quaisquer dos seguintes documentos: c.1. extrato da conta do INSS e do FGTS de qualquer empregado, a critério do CFC; c.2. cópia da folha de pagamento analítica de qualquer mês da prestação dos serviços, em que conste como tomador o CFC; c.3. cópia dos contracheques dos empregados relativos a qualquer mês da prestação dos serviços ou, ainda, quando necessário, cópia de recibos de depósitos bancários; c.4. comprovantes de entrega de benefícios suplementares (vale-transporte, vale-alimentação, entre outros), a que estiver obrigada por força de lei ou de Convenção ou Acordo Coletivo de Trabalho, relativos a qualquer mês da prestação dos serviços e de qualquer empregado; e c.5. comprovantes de realização de eventuais cursos de treinamento e reciclagem que forem exigidos por lei ou pelo contrato.	Primeiro mês da prestação dos serviços
d) entregar cópia da documentação abaixo relacionada, quando da extinção ou rescisão do contrato, após o último mês de prestação dos serviços, no prazo definido no contrato: d.1. termos de rescisão dos contratos de trabalho dos empregados prestadores de serviço, devidamente homologados, quando exigível pelo sindicato da categoria; d.2. guias de recolhimento da contribuição previdenciária e do FGTS, referentes às rescisões contratuais; d.3. extratos dos depósitos efetuados nas contas vinculadas individuais do FGTS de cada empregado dispensado; d.4. exames médicos demissionais dos empregados dispensados.	Após o último mês de prestação dos serviços, quando da extinção ou rescisão do contrato.

b.1. Certidão Negativa de Débitos relativos a Créditos Tributários Federais e à Dívida Ativa da União (CND); b.2. certidões que comprovem a regularidade perante as Fazendas Estadual, Distrital e Municipal do domicílio ou sede da Contratada; b.3. Certidão de Regularidade do FGTS (CRF); e b.4. Certidão Negativa de Débitos Trabalhistas (CNDT).	Até o dia 30 (trinta) do mês seguinte ao da prestação dos serviços ao setor responsável pela fiscalização do contrato, quando não for possível a verificação da regularidade destes no Sistema de Cadastro de Fornecedores (SICAF)

8. CLASSIFICAÇÃO DOS SERVIÇOS

8.1. O serviço a ser contratado enquadra-se na classificação de serviços comuns, nos termos da Lei nº 10.520, de 2002 e do Decreto nº 3.555, de 2000.

8.2. A natureza dos serviços possui caráter continuado e serão contratados mediante a modalidade Pregão. A modalidade adotada observa, ainda, o disposto no Acórdão nº 2.471/2008 do Tribunal de Contas da União (TCU).

8.3. Os serviços serão prestados de forma contínua, nos horários e jornadas especificados neste Termo de Referência, por mais de um exercício financeiro, visando assegurar a manutenção das atividades acessórias, instrumentais ou auxiliares e não ligadas diretamente à atividade-fim do CFC, enquadrando-se, portanto, nos pressupostos do Decreto nº 9.507/2018 e Art. 15 da IN MPDG/SG nº 5/2017. Caso o horário de expediente do CFC seja alterado por instrumento normativo ou imposição de circunstâncias supervenientes, deverá ser promovida a adequação nos horários da prestação de serviços para atendimento da nova situação.

8.4. Os serviços a serem contratados enquadram-se nos pressupostos do Decreto nº 9.507, de 2018, caracterizando-se como atividades materiais acessórias, instrumentais ou complementares à área de competência legal do órgão licitante, não inerentes às categorias funcionais abrangidas por seu respectivo plano de cargos.

8.5. A prestação dos serviços não gera vínculo empregatício entre os empregados da Contratada e da Administração, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

9. OBRIGAÇÕES DA CONTRATADA

9.1. São obrigações da Contratada:

9.1.1. Executar os serviços conforme especificações do Termo de Referência e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais.

9.1.2. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados.

9.1.3. Manter a execução do serviço nos horários fixados pelo CFC.

9.1.4. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado ao CFC, devendo ressarcir imediatamente a Administração em sua integralidade, ficando a Contratante autorizada a descontar da garantia, exigida no edital, ou dos pagamentos devidos à Contratada, o valor correspondente aos danos sofridos.

9.1.5. Utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, de conformidade com as normas e determinações em vigor.

9.2. Vedar a utilização, na execução dos serviços, de empregado que seja familiar de funcionário ou ocupante de cargo em comissão ou função de confiança ou conselheiros do CFC, nos termos do artigo 7º do Decreto nº 7.203, de 2010.

9.3. Disponibilizar à Contratante os empregados devidamente identificados por meio de crachá.

9.4. As empresas contratadas que sejam regidas pela Consolidação das Leis do Trabalho (CLT) deverão apresentar a seguinte documentação no primeiro mês de prestação dos serviços, conforme alínea "g" do item 10.1 do Anexo VIII-B da IN SEGES/MP N. 5/2017:

9.4.1. Relação dos empregados, contendo nome completo, cargo ou função, salário, horário do posto de trabalho, números da carteira de identidade (RG) e da inscrição no Cadastro de Pessoas Físicas (CPF), com indicação dos responsáveis técnicos pela execução dos serviços, quando for o caso;

9.4.2. Carteira de Trabalho e Previdência Social (CTPS) dos empregados admitidos e dos responsáveis técnicos pela execução dos serviços, quando for o caso, devidamente assinada pela Contratada;

9.4.3. Exames médicos admissionais dos empregados da contratada que prestarão os serviços;

9.4.4. Declaração de responsabilidade exclusiva da contratada sobre a quitação dos encargos trabalhistas e sociais decorrentes do contrato;

9.4.5. Os documentos acima mencionados deverão ser apresentados para cada novo empregado que se vincule à prestação do contrato administrativo. De igual modo, o desligamento de empregados no curso do contrato de prestação de serviços deve ser devidamente comunicado, com toda a documentação pertinente ao empregado dispensado, à semelhança do que se exige quando do encerramento do contrato administrativo.

9.5. Apresentar relação mensal dos empregados que expressamente optarem por não receber o vale transporte.

9.6. Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, a empresa contratada cujos empregados vinculados ao serviço sejam regidos pela CLT deverá entregar ao setor responsável pela fiscalização do contrato, até o dia trinta do mês seguinte ao da prestação dos serviços, os seguintes documentos:

- a) prova de regularidade relativa à Seguridade Social;
- b) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União;
- c) certidões que comprovem a regularidade perante as Fazendas Distrital e Municipal do domicílio ou sede da Contratado;
- d) certidão de Regularidade do FGTS – CRF; e
- e) certidão Negativa de Débitos Trabalhistas – CNDT, conforme alínea "c" do item 10.2 do Anexo VIII-B da IN SEGES/MP n. 5/2017.

9.7. Substituir, no prazo de 3 (três) horas, em caso de eventual ausência, tais como faltas e licenças, o empregado posto a serviço da Contratante, devendo identificar previamente o respectivo substituto ao Fiscal do Contrato.

9.8. Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato, por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade à Contratante.

9.8.1. Não serão incluídas nas planilhas de custos e formação de preços as disposições contidas em Acordos, Dissídios ou Convenções Coletivas que tratem de pagamento de participação dos trabalhadores nos lucros ou resultados da empresa contratada, de matéria não trabalhista, de obrigações e direitos que somente se aplicam aos contratos com a Administração Pública, ou que estabeleçam direitos não previstos em lei, tais como valores ou índices obrigatórios de encargos sociais ou previdenciários, bem como de preços para os insumos relacionados ao exercício da atividade.

9.9. Efetuar o pagamento dos salários dos empregados alocados na execução contratual mediante depósito na conta bancária de titularidade do trabalhador, em agência situada na localidade ou região metropolitana em que ocorre a prestação dos serviços, de modo a possibilitar a conferência do pagamento por parte da Contratante. Em caso de impossibilidade de cumprimento desta disposição, a Contratada deverá apresentar justificativa, a fim de que o CFC analise sua plausibilidade e possa verificar a realização do pagamento.

9.10. Autorizar o CFC, no momento da assinatura do contrato, a fazer o desconto nas faturas e realizar os pagamentos dos salários e demais verbas trabalhistas diretamente aos trabalhadores, bem como das contribuições previdenciárias e do FGTS, quando não demonstrado o cumprimento tempestivo e regular dessas obrigações, até o momento da regularização, sem prejuízo das sanções cabíveis.

9.10.1. Quando não for possível a realização desses pagamentos pela própria Administração (ex.: por falta da documentação pertinente, tais como folha de pagamento, rescisões dos contratos e guias de recolhimento), os valores retidos cautelarmente serão depositados junto à Justiça do Trabalho, com o objetivo de serem utilizados exclusivamente no pagamento de salários e das demais verbas trabalhistas, bem como das contribuições sociais e FGTS decorrentes.

9.11. Atender às solicitações da Contratante quanto à substituição dos empregados alocados, no prazo fixado pelo fiscal do contrato, nos casos em que ficar constatado descumprimento das obrigações relativas à execução do serviço, conforme descrito neste Termo de Referência.

9.12. Instruir seus empregados quanto à necessidade de acatar as Normas Internas do CFC.

9.13. Instruir seus empregados a respeito das atividades a serem desempenhadas, alertando-os a não executar atividades não abrangidas pelo contrato, devendo a Contratada relatar à Contratante toda e qualquer ocorrência neste sendo, a fim de evitar desvio de função.

9.14. Instruir seus empregados, no início da execução contratual, quanto à obtenção das informações de seus interesses junto aos órgãos públicos, relativas ao contrato de trabalho e obrigações a ele inerentes, adotando, entre outras, as seguintes medidas:

9.14.1. viabilizar o acesso de seus empregados, via internet, por meio de senha própria, aos sistemas da Previdência Social e da Receita Federal do Brasil, com o objetivo de verificar se as suas contribuições previdenciárias foram recolhidas, no prazo máximo de 60 (sessenta) dias, contados do início da prestação dos serviços ou da admissão do empregado;

9.14.2. viabilizar a emissão do cartão cidadão pela Caixa Econômica Federal para todos os empregados, no prazo máximo de 60 (sessenta) dias, contados do início da prestação dos serviços ou da admissão do empregado;

9.14.3. oferecer todos os meios necessários aos seus empregados para a obtenção de extratos de recolhimentos de seus direitos sociais, preferencialmente por meio eletrônico, quando disponível.

9.15. Formalizar a indicação de preposto da empresa e substituto eventual para a coordenação dos serviços e gestão administrativa do contrato.

9.16. Relatar à Contratante toda e qualquer irregularidade verificada no decorrer da prestação dos serviços.

9.17. Fornecer, sempre que solicitados pela Contratante, os comprovantes do cumprimento das obrigações previdenciárias, do Fundo de Garantia do Tempo de Serviço (FGTS), e do pagamento dos salários e demais benefícios trabalhistas dos empregados colocados à disposição da Contratante.

9.17.1. A ausência da documentação pertinente ou da comprovação do cumprimento das obrigações trabalhistas, previdenciárias e relativas ao FGTS implicará a retenção do pagamento da fatura mensal, em valor proporcional ao inadimplemento, mediante prévia comunicação, até que a situação seja regularizada, sem prejuízo das demais sanções cabíveis.

9.17.2. Ultrapassado o prazo de 15 (quinze) dias, contados na comunicação mencionada no subitem anterior, sem a regularização da falta, o CFC poderá efetuar o pagamento das obrigações diretamente aos empregados da Contratada que tenham participado da execução dos serviços objeto do contrato, sem prejuízo das demais sanções cabíveis.

9.17.2.1. O sindicato representante da categoria do trabalhador deverá ser notificado pela contratante para acompanhar o pagamento das respectivas verbas.

- 9.18. Não permitir a utilização de qualquer trabalho do menor de 16 (dezesesseis) anos, exceto na condição de aprendiz para os maiores de 14 (quatorze anos); nem permitir a utilização do trabalho do menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre.
- 9.19. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.
- 9.20. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato.
- 9.21. Não beneficiar-se da condição de optante pelo Simples Nacional, salvo as exceções previstas no § 5º-C do art. 18 da Lei Complementar nº 123, de 14 de dezembro de 2006.
- 9.22. Comunicar formalmente à Receita Federal do Brasil a assinatura do contrato de prestação de serviços mediante cessão de mão de obra, salvo as exceções previstas no § 5º-C do art. 18 da Lei Complementar nº 123, de 14 de dezembro de 2006, para fins de exclusão obrigatória do Simples Nacional a contar do mês seguinte ao da contratação, conforme previsão do art.17, XII, art. 30, §1º, II e do art. 31, II, todos da Lei Complementar nº 123, de 2006.
- 9.22.1. Para efeito de comprovação da comunicação, a Contratada deverá apresentar cópia do ofício enviado à Receita Federal do Brasil, com comprovante de entrega e recebimento, comunicando a assinatura do contrato de prestação de serviços mediante cessão de mão de obra, até o último dia útil do mês subsequente ao da ocorrência da situação de vedação.
- 9.23. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, tais como os valores providos com o quantitativo de vale transporte, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do § 1º do art. 57 da Lei nº 8.666, de 1993.
- 9.24. Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços.
- 9.25. Prestar todo esclarecimento ou informação solicitada pela Contratante ou por seu preposto, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do serviço.
- 9.26. Paralisar, por determinação do CFC, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.
- 9.27. Promover a guarda, manutenção e vigilância de equipamentos, materiais, ferramentas, e tudo o que for necessário à execução dos serviços, durante a vigência do contrato.
- 9.28. Promover a organização técnica e administrativa dos serviços, de modo a conduzi-los eficaz e eficientemente, de acordo com os documentos e especificações que integram este Termo de Referência, no prazo determinado.
- 9.29. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações do CFC, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina.
- 9.30. Submeter previamente, por escrito, à Contratante, para análise e aprovação, qualquer mudança no método de execução do serviço que fuja das especificações constantes deste Termo de Referência.
- 9.31. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança da Contratante.
- 9.32. Disponibilizar os empregados para a Contratante devidamente identificados por crachás, sempre limpos e asseados, quer no aspecto de vestuário e calçado, quer na higiene pessoal, devendo ser substituídos imediatamente àqueles que não estiverem de acordo com esta exigência, mediante comunicação do Fiscal do Contrato.
- 9.33. Orientar regularmente seus empregados acerca da adequada metodologia de otimização dos serviços, dando ênfase à economia no emprego de materiais e a racionalização de energia elétrica e água.
- 9.34. Selecionar e preparar rigorosamente os empregados que irão prestar os serviços, encaminhando profissionais portadores de atestados de boa conduta e demais referências, regularmente registrados nas CTPS.
- 9.35. Manter a disciplina nos locais dos serviços, substituindo, no prazo máximo de 24 (vinte e quatro) horas, após a notificação, qualquer empregado cuja atuação, permanência e/ou comportamento sejam julgados prejudiciais, inconvenientes e/ou insatisfatórios.
- 9.36. Comunicar ao Fiscal do Contrato, no prazo máximo de 24 (vinte e quatro) horas, o desligamento de empregado da Contratada, devendo a substituição ser promovida no mesmo prazo. Os empregados substitutos devem ser orientados sobre as técnicas de execução dos serviços.
- 9.37. Manter sediados junto ao CFC, durante os turnos de trabalho, profissionais capazes de tomar decisões compatíveis com os compromissos assumidos.
- 9.38. Instruir os seus empregados quanto à prevenção de incêndios e acidentes nas áreas do CFC.
- 9.39. Registrar e controlar, juntamente com o fiscal do CFC, diariamente, a assiduidade e a pontualidade de seu pessoal, bem como as ocorrências havidas.
- 9.40. Fazer seguro de seus empregados contra riscos de acidentes de trabalho, responsabilizando-se, também, pelos encargos trabalhistas, previdenciários, fiscais e comerciais, resultantes da execução do contrato, conforme exigência legal.
- 9.41. Acatar as orientações da fiscalização designada pela Contratante, levada a efeito por pessoa devidamente credenciada para tal fim.
- 9.42. Tratar e negociar todo e qualquer assunto relativo à execução do contrato somente com o gestor e/ou o Fiscal do Contrato, sem que haja ingerência de terceiros não credenciados para tal fim.

- 9.43. Fornecer antecipadamente aos seus empregados auxílio-transporte, auxílio alimentação, de acordo com o horário de trabalho, e qualquer outro benefício que se torne necessário ao bom e completo desempenho de suas atividades e de acordo com a legislação vigente.
- 9.44. Instruir os profissionais alocados quanto à necessidade de acatar as orientações do fiscal do CFC, intermediadas por meio d preposto da Contratada, inclusive quanto ao cumprimento das Normas Internas Regimentais e Disciplinares e de Segurança e Medicina do Trabalho, não caracterizando a manutenção de qualquer vínculo empregatício com a Contratante.
- 9.45. Instruir seus empregados a não executarem serviços particulares a pedido de colaboradores do CFC (conselheiros, funcionários, estagiários, aprendizes, cargos comissionados, terceirizados).
- 9.46. Fornecer ao Fiscal do contrato relatório técnico mensal das atividades realizadas, constando relações nominais de licenças, faltas, se houver, bem assim escala nominal de férias dos empregados e seus respectivos substitutos.
- 9.47. Apresentar à contratante, com no mínimo 3 (três) meses de antecedência, escala de férias para fins de avaliação, observada a necessidade de serviços da Contratante.
- 9.48. Assumir todas as responsabilidades e tomar as medidas necessárias ao atendimento dos seus empregados acidentados ou com mal súbito.
- 9.49. Proibir o acesso por parte de seus empregados à internet em sites que não estejam relacionados com o objeto do serviço contratado, sendo permitido somente o acesso aos softwares e aos diretórios relacionados à execução dos trabalhos contratados.
- 9.50. Cumprir todas as obrigações contidas em convenção coletiva, acordo coletivo ou sentença normativa em dissídio coletivo de trabalho.
- 9.51. Responder por danos e desaparecimento de bens materiais, e avarias que venham a ser causados por seus empregados ou preposto, a terceiros ou ao próprio local de serviço, desde que fique comprovada sua responsabilidade, de acordo com o art. 70, da Lei n.º 8.666/93
- 9.52. Não sendo possível a substituição do bem desaparecido, danificado ou extraviado, a Contratante poderá autorizar o ressarcimento em espécie, promovendo previamente, nesta hipótese, a apuração do valor de mercado, atualizado, do bem, para efeito de recolhimento da importância respectiva aos cofres públicos.
- 9.53. Não transferir a outrem no todo ou em parte, o objeto da presente contratação.
- 9.54. Não caucionar ou utilizar o contrato para qualquer operação financeira, sob pena de rescisão contratual.
- 9.55. Responsabilizar-se pelos danos causados ao patrimônio do CFC, por dolo, negligência, imperícia ou imprudência de seus empregados, ficando obrigada a promover a devida restauração e/ou o ressarcimento a preços utilizados, dentro de 30 (trinta) dias contados a partir da comprovação de sua responsabilidade. Caso não o faça dentro do prazo estipulado, o CFC reserva-se o direito de descontar o valor do ressarcimento da fatura do mês, sem prejuízo de poder denunciar o contrato, de pleno direito.
- 9.56. Não vincular o pagamento dos salários e demais vantagens de seus empregados aos pagamentos das faturas pelo CFC.
- 9.57. Orientar seus empregados a adotar medidas para evitar o desperdício de água tratada, redução de consumo de energia elétrica e redução de produção de resíduos sólidos, observadas as normas ambientais vigentes, em especial o que consta no Plano de Logística Sustentável do CFC.
- 9.58. Cumprir e fazer cumprir as regras e procedimentos institucionalizados pelo CFC, tais como: instruções ou orientações de execução dos trabalhos, Código de Conduta para os Conselheiros, Colaboradores e Funcionários dos Conselhos Federal e Regionais de Contabilidade, procedimentos gerais e específicos da ISO, Plano de Logística Sustentável, normas e manuais, sistemas informatizados, entre outros procedimentos que tenham relação com a prestação de serviços.
- 9.58.1. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;
- 9.58.2. Não transferir a terceiros, por qualquer forma, nem mesmo parcialmente, as obrigações assumidas, nem subcontratar qualquer das prestações a que está obrigada, exceto nas condições autorizadas no Termo de Referência ou no Contrato;
- 9.58.3. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, tais como os valores providos com o quantitativo de vale transporte, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento ao objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do § 1º do art. 57 da Lei nº 8.666, de 1993.
- 9.59. A empresa poderá fornecer junto com a proposta encaminhada para fins de comprovação de atendimento das especificações técnica o **ANEXO VIII - COMPROVAÇÃO TÉCNICA**, para agilizar o processo de análise de documentação.
- 9.60. Após assinatura de contrato a empresa contratada deverá encaminhar os certificados de **COMPETÊNCIAS TÉCNICAS** listados de acordo com o serviço constantes nos itens **4 e 5 do ANEXO I** deste termo de referência.

10. OBRIGAÇÕES DA CONTRATANTE

- 10.1. São obrigações da Contratante:
- 10.1.1. Proporcionar todas as condições para que a Contratada possa desempenhar seus serviços de acordo com as determinações do Contrato, do Edital e seus Anexos, especialmente do Termo de Referência;
- 10.1.2. Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta;
- 10.1.3. Exercer o acompanhamento e a fiscalização dos serviços, pelo Gerente do Departamento de Informática do CFC ou pelo substituto, quando da ausência do mesmo, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o

nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;

10.1.4. Notificar a Contratada por escrito da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção;

10.1.5. Não permitir que os empregados da Contratada realizem horas extras, exceto em caso de comprovada necessidade de serviço, formalmente justificada pela autoridade do órgão para o qual o trabalho seja prestado e desde que observado o limite da legislação trabalhista;

10.1.6. Pagar à Contratada o valor resultante da prestação do serviço, na forma do contrato;

10.1.7. Zelar para que durante toda a vigência do contrato sejam mantidas, em compatibilidade com as obrigações assumidas pela Contratada, todas as condições de habilitação e qualificação exigidas na licitação;

10.1.8. Não praticar atos de ingerência na administração da Contratada, tais como:

10.1.8.1. Exercer o poder de mando sobre os empregados da Contratada, devendo reportar-se somente aos prepostos ou responsáveis por ela indicados, exceto quando o objeto da contratação prever o atendimento direto, tais como nos serviços de recepção e apoio ao usuário;

10.1.8.2. Direcionar a contratação de pessoas para trabalhar nas empresas contratadas;

10.1.8.3. Promover ou aceitar o desvio de funções dos trabalhadores da Contratada, mediante a utilização destes em atividades distintas daquelas previstas no objeto da contratação e em relação à função específica para a qual o trabalhador foi contratado; e

10.1.8.4. Considerar os trabalhadores da Contratada como colaboradores eventuais do próprio órgão ou entidade responsável pela contratação, especialmente para efeito de concessão de diárias e passagens.

11. INÍCIO DOS SERVIÇOS

11.1. Após a assinatura do contrato, o CFC convocará a reunião inicial para alinhamento de expectativas contratuais, a ser realizada no prazo máximo de 10 (dez) dias úteis, contados da data de assinatura do contrato. A reunião deverá contar com a participação, no mínimo: do fiscal técnico e gestor do contrato designados pelo CFC, do representante legal da Contratada, do preposto da Contratada e do gerente de contrato da Contratada, caso esse papel não seja acumulado pelo preposto.

11.2. A pauta da reunião inicial do contrato deverá contemplar, no mínimo, os seguintes pontos:

11.2.1. Apresentação dos participantes;

11.2.2. Entrega, por parte da Contratada, do termo de compromisso contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes no CFC, conforme modelos constantes no Anexo III, a serem assinados pelo representante legal da Contratada;

11.2.3. Esclarecimentos relativos a questões operacionais, administrativas e de gerenciamento do contrato.

11.3. A não realização, por parte da Contratada, das atividades descritas neste item configura inexecução total do contrato, o que sujeita a Contratada às sanções previstas no mesmo.

12. CONDIÇÃO PARA A EXECUÇÃO DOS SERVIÇOS

12.1. Será de responsabilidade da Contratada, para garantir a celeridade e a qualidade da prestação dos serviços, manter à disposição do CFC os profissionais (com experiência e capacidade técnica) para cumprimento das atividades, de acordo com o disposto neste Termo de Referência.

12.2. A Contratante poderá, de acordo com a qualidade do serviço prestado, solicitar a substituição de profissionais da equipe por outros que atendam aos requisitos técnicos, de formação e de experiência exigidos neste Termo de Referência.

12.3. Os profissionais deverão atuar exclusivamente na execução dos serviços contratados durante a jornada de trabalho, não sendo admitido o compartilhamento de tempo com atividades alheias ao objeto do contrato.

12.4. A Contratada deverá formalizar a indicação de preposto da empresa e substituto eventual para a coordenação dos serviços e suporte administrativo inerente às atividades a serem executadas, garantido um serviço de alto padrão, sem nenhum custo adicional para o CFC.

12.5. O especificado no item 12.4 diz respeito a:

a) Gerenciamento do contrato;

b) Gerenciamento do pessoal local e remotamente;

c) Controle das atividades desenvolvidas pelos profissionais;

d) Gerenciamento de contingência na manutenção da execução ininterrupta dos serviços;

e) Gerenciamento e política de segurança a ser adotada pela Contratada para garantir e manter o sigilo e a integridade das informações acessadas pelos profissionais; e

f) Gerenciamento do conhecimento dos serviços executados para o seu repasse em caso de substituição.

12.6. A licitante deverá considerar, na composição do encargo mensal ofertado, a cobertura de todos os dispêndios envolvidos e de suas responsabilidades, tais como, salário dos profissionais alocados e seus encargos trabalhistas, além de impostos e demais encargos fiscais.

12.7. Para viabilizar a fiscalização pela Contratante, as contratações e demissões ocorridas no âmbito do contrato deverão ser informadas previamente ao CFC. Além disso, quando da substituição dos profissionais, a Contratada deverá observar os requisitos de qualificação previstos e deverá encaminhar ao CFC documentação que comprove o atendimento a tais requisitos.

13. REQUISITOS MÍNIMOS DE HABILITAÇÃO TÉCNICA

13.1. A exigência de comprovação de capacidade técnica relacionada ao objeto licitado se dá com base no art. 30, § 1º, da Lei nº 8.666/93, e visa garantir que a licitante já forneceu os serviços exigidos neste Edital e, portanto, possui capacidade técnico-operacional para fornecê-lo adequadamente.

13.1.1. ATESTADOS DE CAPACIDADE TÉCNICA:

13.1.2. A LICITANTE deverá fornecer obrigatoriamente, além das qualificações exigidas os seguintes atestados ou declarações de capacidade técnica, expedido por pessoa jurídica de direito público ou privado, que comprove ter a licitante prestado serviços compatíveis com o objeto da licitação:

13.1.3. Atestado de realização de diagnóstico e apoio à implantação de conformidade com a LGPD (Lei Geral de Proteção de Dados) para instituição com 500 ou mais funcionários.

13.1.4. SERVIÇOS GERENCIADOS DE SEGURANÇA em regime de 24 (vinte quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano com as seguintes parcelas de maior relevância:

13.1.5. Serviços Gerenciados de Segurança (MSS – Managed Security Services) por meio de 2 (dois) SOC (Security Operation Center) redundantes. Esses centros devem utilizar ou ter utilizado 2 (duas) infraestruturas de datacenters, podendo estarem situadas fora dos ambientes de SOC (Security Operation Center). Os Serviços Gerenciados de Segurança devem ter incluído a execução de processos de monitoramento, detecção, triagem, tratamento e resposta a incidentes de segurança, utilizando tecnologia de SIEM (Security Information and Event Management) para gerenciamento e correlação de eventos de segurança, em redes com, no mínimo, 200 (duzentas) estações de trabalho, incluindo desktops e notebooks.

13.1.6. Serviços de Firewall, por meio do fornecimento e instalação de equipamentos ou prestação de serviços de suporte ou assistência técnica, em redes com, no mínimo, 259 (duzentos e cinquenta e nove) estações de trabalho, incluindo desktops e notebooks;

13.1.6.1. A exigência da comprovação mínima de 259 (duzentos e cinquenta e nove) equipamentos que representa de 50% (cinquenta por cento) das estações de trabalho, Notebook ou Netbook do item 4.1.3 totalizando de 518 do parque atual.

13.1.6.2. Fórmula aplicada $518 \times 50\% = 259$.

13.1.7. Serviços de Administração e Monitoramento de Segurança, por meio do fornecimento e instalação de equipamentos ou prestação de serviços de administração e monitoramento de segurança em redes com, no mínimo, 259 (duzentos e cinquenta e nove) ativos de TI;

13.1.7.1. A exigência da comprovação mínima de 259 (duzentos e cinquenta e nove) equipamentos que representa de 50% (cinquenta por cento) das estações de trabalho, Notebook ou Netbook do item 4.1.3 totalizando de 518 do parque atual.

13.1.7.2. Fórmula aplicada $518 \times 50\% = 259$.

13.1.8. Serviços de respostas aos incidentes de segurança e de privacidade, por meio do fornecimento e instalação de equipamentos ou prestação de serviços de respostas a incidentes de segurança em redes com, no mínimo, 200 (duzentos) ativos de TI ou 200 (duzentos) funcionários;

13.1.9. Serviço de Gestão de Vulnerabilidades, por meio do fornecimento e instalação de equipamentos ou prestação de serviços de suporte ou assistência técnica, os quais devem monitorar e tratar, no mínimo, 200 (duzentos) ativos de TI;

13.1.10. Os serviços supracitados podem estar distribuídos em diversos atestados de capacidade técnica, não se exigindo que todos sejam prestados a uma única pessoa jurídica de direito público ou privado;

13.1.11. O Conselho Federal de Contabilidade poderá promover a qualquer tempo diligência para checar a veracidade das informações dos documentos comprobatórios do conteúdo declarado.

13.1.12. Todos os atestados apresentados na documentação de habilitação deverão conter, obrigatoriamente, a especificação dos serviços executados, o nome e cargo do declarante.

13.1.13. O não atendimento às especificações técnicas descritas neste Termo de Referência implicará na desclassificação da proposta apresentada.

13.2. DECLARAÇÃO DE NOC – NETWORK OPERATION CENTER:

13.2.1. A LICITANTE deverá apresentar declaração, datada e assinada por seu representante legal, de que possui Centros de operação de Rede (NOC), para a realização dos serviços de Suporte técnico, monitoramento e operação, atendendo no mínimo as seguintes características:

13.2.2. Deve operar em regime 24x7 durante todos os dias do ano por toda a duração do contrato;

13.2.3. Possui Energia e no-breaks redundantes;

13.2.4. Possui possuir Grupo gerador;

13.2.5. Possui possuir canais redundantes de comunicação IP dedicados com a Internet, com provedores distintos, com SLA de atendimento igual ou inferior a 04 (quatro) horas para o caso de queda do link. Não serão aceitos contratos com links xDSL, devido ao baixo SLA ofertado pelas operadoras de telecomunicação para este tipo de tecnologia;

- 13.2.6. Possui Sistemas de refrigeração redundantes;
- 13.2.7. Possui Sistema de monitoramento por câmeras;
- 13.2.8. Possui Sistemas de monitoramento e alarme contra incêndio;
- 13.2.9. Possui Firewalls redundantes;
- 13.2.10. Possui Switches redundantes;
- 13.2.11. Possui Roteadores redundantes; e
- 13.2.12. Possui Servidores e Blades redundantes para prover os serviços contratados;
- 13.2.13. Essas especificações poderão ser comprovadas através de diligência;

14. VISTORIA FACULTATIVA

- 14.1. Para o correto dimensionamento e elaboração de sua proposta, será facultado à empresa interessada conhecer o ambiente computacional e as instalações do Contratante. Para tanto, poderá ser agendada vistoria técnica ao ambiente do Contratante, no prazo de até 1 (um) dia útil antes da data de realização do pregão eletrônico.
- 14.2. A vistoria deverá ser agendada por meio do telefone (61) 3314-9441, mencionando o número do Edital, o objeto, a razão social, endereço e telefone da empresa interessada além do nome completo, telefone do representante encarregado de realizar a vistoria. As vistorias serão agendadas nos horários de 09:00 às 12:00h e das 14:00 às 17:00h, de segunda a sexta-feira, de acordo com a disponibilidade do CFC.
- 14.3. Para a vistoria, a Licitante, ou o seu representante, deverá estar devidamente identificado e usando as proteções devido ao COVID 19.
- 14.4. A vistoria técnica deverá ser realizada por representante legal da Licitante, o qual deverá portar original ou cópia autenticada do contrato social da empresa, procuração autenticada em cartório para representar a empresa interessada, e documento de identificação pessoal original com foto, a serem apresentados aos servidores do Conselho Federal.
- 14.5. Para todos os efeitos, considerar-se-á que a Licitante, optante pela realização de vistoria ou não, tem pleno conhecimento da natureza e do escopo dos serviços, não se admitindo, posteriormente, qualquer alegação de desconhecimento dos serviços e de dificuldades técnicas não previstas.
- 14.6. Quaisquer dúvidas com relação à vistoria deverão ser sanadas na própria vistoria.
- 14.7. O Contratante se reserva ao direito de designar terceiros para acompanhar as vistorias técnicas.
- 14.8. Os custos decorrentes destas vistorias ocorrerão a cargo da empresa interessada.

15. COMPROVAÇÃO TÉCNICA

- 15.1. No momento da entrega da proposta:
- 15.1.1. A licitante poderá apresentar comprovação de atendimento às especificações técnicas descritas neste Termo de Referência, conforme o Anexo VIII juntamente com a proposta, para agilizar o processo de análise de documentação.
- 15.2. Após assinatura do contrato:
- 15.2.1. Encaminhar lista de certificados de **COMPETÊNCIAS TÉCNICAS** conforme subitem 9.60.

16. QUALIFICAÇÃO ECONÔMICO-FINANCEIRA

- 16.1. Certidão negativa de falência expedida pelo distribuidor da sede do licitante.
- 16.1.1. Para as certidões que não trouxerem expresso o prazo de validade, considerar-se-á 90 (noventa) dias da data da sua expedição.
- 16.2. Comprovação da boa situação financeira:
- 16.2.1. Índices de Liquidez Geral (LG), Liquidez Corrente (LC) e Solvência Geral (SG) superiores a 1 (um), índices calculados com base nas demonstrações contábeis, obtidos pela aplicação das seguintes fórmulas:
 - LG = Ativo Circulante + Realizável a Longo Prazo / Passivo Circulante + Passivo Não Circulante
 - SG = Ativo Total / Passivo Circulante + Passivo Não Circulante
 - LC = Ativo Circulante / Passivo Circulante.
- 16.2.2. As empresas, cadastradas ou não no SICAF, que apresentarem resultado inferior ou igual a 1(um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverão comprovar patrimônio líquido de 10% (dez por cento) do valor estimado da contratação ou do item pertinente.
- 16.2.3. Comprovação de possuir Capital Circulante Líquido (CCL) ou Capital de Giro (Ativo Circulante – Passivo Circulante) de, no mínimo, 16,66% (dezesseis inteiros e sessenta e seis centésimos por cento) do valor estimado para a contratação ou item pertinente, tendo por base o balanço patrimonial e as demonstrações contábeis já exigíveis na forma da lei;
- 16.2.4. Comprovação de patrimônio líquido de 10% (dez por cento) do valor estimado da contratação, tendo por base o balanço patrimonial do último exercício social.

16.2.5. Comprovação, por meio de declaração, da relação de compromissos assumidos, conforme modelo constante do Anexo X, de que 1/12 (um doze avos) do valor total dos contratos firmados com a Administração Pública e/ou com a iniciativa privada, vigentes na data da sessão pública de abertura deste Pregão, não é superior ao Patrimônio Líquido do licitante, podendo este ser atualizado.

16.2.5.1. Quando houver divergência percentual superior a 10% (dez por cento), para mais ou para menos, entre a declaração aqui tratada e a receita bruta discriminada na Demonstração do Resultado do Exercício (DRE), deverão ser apresentadas, concomitantemente, as devidas justificativas.

16.2.6. A licitante deverá apresentar declaração assinada por profissional habilitado da área contábil, que ateste o atendimento pelo licitante dos índices econômicos previstos neste Termo de Referência.

17. SUBCONTRATAÇÃO

17.1. Não será admitida a subcontratação para fornecimento dos serviços exigidos do objeto licitatório.

18. ALTERAÇÃO SUBJETIVA

18.1. É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa do Conselho Federal de Contabilidade à continuidade do contrato.

19. CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO DOS SERVIÇOS

19.1. O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da prestação dos serviços, dos materiais, técnicas e equipamentos empregados, de forma a assegurar o perfeito cumprimento do ajuste, que serão exercidos por um ou mais representantes da Contratante, especialmente designados, na forma dos arts. 67 e 73 da Lei nº 8.666, de 1993.

19.2. As atividades de gestão e fiscalização da execução contratual são o conjunto de ações que tem por objetivo aferir o cumprimento dos resultados previstos pela Administração para o serviço contratado, verificar a regularidade das obrigações previdenciárias, fiscais e trabalhistas, bem como prestar apoio à instrução processual e o encaminhamento da documentação pertinente ao Departamento de Licitação e Contratos (Delic) para a formalização dos procedimentos relativos a repactuação, alteração, reequilíbrio, prorrogação, pagamento, eventual aplicação de sanções, extinção do contrato, dentre outras, com vista a assegurar o cumprimento das cláusulas avençadas e a solução de problemas relativos ao objeto.

19.3. O conjunto de atividades de gestão e fiscalização compete ao gestor da execução do contrato, podendo ser auxiliado pela fiscalização técnica, administrativa, setorial e pelo público usuário, de acordo com as seguintes disposições:

I – Gestão da Execução do Contrato: é a coordenação das atividades relacionadas à fiscalização técnica, administrativa, setorial e pelo público usuário, bem como dos atos preparatórios à instrução processual e ao encaminhamento da documentação pertinente ao Departamento de Licitação e Contratos (Delic) para formalização dos procedimentos quanto aos aspectos que envolvam a prorrogação, alteração, reequilíbrio, pagamento, eventual aplicação de sanções, extinção do contrato, dentre outros;

II – Fiscalização Técnica: é o acompanhamento com o objetivo de avaliar a execução do objeto nos moldes contratados e, se for o caso, aferir se a quantidade, qualidade, tempo e modo da prestação dos serviços estão compatíveis com os indicadores de níveis mínimos de desempenho estipulados no ato convocatório, para efeito de pagamento conforme o resultado, podendo ser auxiliado pela fiscalização e público usuário;

III – Fiscalização Administrativa: é o acompanhamento dos aspectos administrativos da execução dos serviços, quanto às obrigações previdenciárias, fiscais e trabalhistas, bem como quanto às providências tempestivas nos casos de inadimplemento.

19.4. As atividades de gestão e fiscalização da execução contratual devem ser realizadas de forma preventiva, rotineira e sistemática, podendo ser exercidas por empregados, equipe de fiscalização ou único empregado, desde que, no exercício dessas atribuições, fique assegurada a distinção dessas atividades e, em razão do volume de trabalho, não comprometa o desempenho de todas as ações relacionadas à Gestão do Contrato.

19.5. A fiscalização administrativa poderá ser efetivada com base em critérios estatísticos, levando-se em consideração falhas que impactem o contrato como um todo e não apenas erros e falhas eventuais no pagamento de alguma vantagem a um determinado empregado.

19.6. Na fiscalização do cumprimento das obrigações trabalhistas e sociais exigir-se-á, dentre outras, as seguintes comprovações (os documentos poderão ser originais ou cópias autenticadas por cartório competente ou por funcionário do CFC), no caso de empresas regidas pela Consolidação das Leis do Trabalho (CLT):

a) no primeiro mês da prestação dos serviços, a Contratada deverá apresentar a seguinte documentação:

a.1. relação dos empregados, contendo nome completo, cargo ou função, horário do posto de trabalho, números da carteira de identidade (RG) e da inscrição no Cadastro de Pessoas Físicas (CPF), com indicação dos responsáveis técnicos pela execução dos serviços, quando for o caso;

a.2. Carteira de Trabalho e Previdência Social (CTPS) dos empregados admitidos e dos responsáveis técnicos pela execução dos serviços, quando for o caso, devidamente assinada pela Contratada; e

a.3. exames médicos admissionais dos empregados da Contratada que prestarão os serviços.

b) entrega até o dia trinta do mês seguinte ao da prestação dos serviços ao setor responsável pela fiscalização do

contrato dos seguintes documentos, quando não for possível a verificação da regularidade destes no Sistema de Cadastro de Fornecedores (SICAF):

- b.1. Certidão Negativa de Débitos relativos a Créditos Tributários Federais e à Dívida Ativa da União (CND);
- b.2. certidões que comprovem a regularidade perante as Fazendas Estadual, Distrital e Municipal do domicílio ou sede da Contratada;
- b.3. Certidão de Regularidade do FGTS (CRF); e
- b.4. Certidão Negativa de Débitos Trabalhistas (CNDT).
- c) entrega, quando solicitado pelo CFC, de quaisquer dos seguintes documentos:
 - c.1. extrato da conta do INSS e do FGTS de qualquer empregado, a critério do CFC;
 - c.2. cópia da folha de pagamento analítica de qualquer mês da prestação dos serviços, em que conste como tomador o CFC;
 - c.3. cópia dos contracheques dos empregados relativos a qualquer mês da prestação dos serviços ou, ainda, quando necessário, cópia de recibos de depósitos bancários;
 - c.4. comprovantes de entrega de benefícios suplementares (vale-transporte, vale-alimentação, entre outros), a que estiver obrigada por força de lei ou de Convenção ou Acordo Coletivo de Trabalho, relativos a qualquer mês da prestação dos serviços e de qualquer empregado; e
 - c.5. comprovantes de realização de eventuais cursos de treinamento e reciclagem que forem exigidos por lei ou pelo contrato.
- d) entrega de cópia da documentação abaixo relacionada, quando da extinção ou rescisão do contrato, após o último mês de prestação dos serviços, no prazo definido no contrato:
 - d.1. termos de rescisão dos contratos de trabalho dos empregados prestadores de serviço, devidamente homologados, quando exigível pelo sindicato da categoria;
 - d.2. guias de recolhimento da contribuição previdenciária e do FGTS, referentes às rescisões contratuais;
 - d.3. extratos dos depósitos efetuados nas contas vinculadas individuais do FGTS de cada empregado dispensado;
 - d.4. exames médicos demissionais dos empregados dispensados.
- 19.7. O CFC deverá analisar a documentação solicitada na alínea “d” acima no prazo de 30 (trinta) dias após o recebimento dos documentos, prorrogáveis por mais 30 (trinta) dias, justificadamente.
- 19.8. No caso de sociedades diversas, tais como as Organizações Sociais, será exigida a comprovação de atendimento a eventuais obrigações decorrentes da legislação que rege as respectivas organizações.
- 19.9. Sempre que houver admissão de novos empregados pela Contratada, os documentos elencados no subitem 18.6 acima deverão ser apresentados.
- 19.10. Em caso de indício de irregularidade no recolhimento das contribuições previdenciárias, os fiscais ou gestores do contrato deverão oficializar à Receita Federal do Brasil (RFB).
- 19.11. Em caso de indício de irregularidade no recolhimento da contribuição para o FGTS, os fiscais ou gestores do contrato deverão oficializar ao Ministério do Trabalho.
- 19.12. O descumprimento das obrigações trabalhistas ou a não manutenção das condições de habilitação pela Contratada poderá dar ensejo à rescisão contratual, sem prejuízo das demais sanções.
- 19.13. O CFC poderá conceder prazo para que a Contratada regularize suas obrigações trabalhistas ou suas condições de habilitação, sob pena de rescisão contratual, quando não identificar má-fé ou a incapacidade de correção.
- 19.14. Além das disposições acima citadas, a fiscalização administrativa observará, ainda, as seguintes diretrizes:
 - 19.14.1. Fiscalização inicial (no momento em que a prestação de serviços é iniciada):
 - a) Será elaborada planilha-resumo de todo o contrato administrativo, com informações sobre todos os empregados terceirizados que prestam serviços, com os seguintes dados: nome completo, número de inscrição no CPF, função exercida, salário, adicionais, gratificações, benefícios recebidos, sua especificação e quantidade (vale-transporte, auxílio-alimentação), horário de trabalho, férias, licenças, faltas, ocorrências e horas extras trabalhadas;
 - b) Todas as anotações contidas na CTPS dos empregados serão conferidas, a fim de que se possa verificar se as informações nelas inseridas coincidem com as informações fornecidas pela contratada e pelo empregado;
 - c) O número de terceirizados por função deve coincidir com o previsto no contrato administrativo;
 - d) O salário não pode ser inferior ao previsto no contrato administrativo e na Convenção Coletiva de Trabalho da Categoria (CCT);
 - e) Serão consultadas eventuais obrigações adicionais constantes na CCT para a Contratada;
 - f) No primeiro mês da prestação dos serviços, a Contratada deverá apresentar a seguinte documentação:
 - f.1. relação dos empregados, com nome completo, cargo ou função, horário do posto de trabalho, números da carteira de identidade (RG) e inscrição no Cadastro de Pessoas Físicas (CPF), e indicação dos responsáveis técnicos pela execução dos serviços, quando for o caso;
 - f.2. CTPS dos empregados admitidos e dos responsáveis técnicos pela execução dos serviços, quando for o caso,

devidamente assinadas pela Contratada;

f.3. exames médicos admissionais dos empregados da Contratada que prestarão os serviços; e

f.4. declaração de responsabilidade exclusiva da contratada sobre a quitação dos encargos trabalhistas e sociais decorrentes do contrato.

19.15. Fiscalização mensal (a ser feita antes do pagamento da fatura):

a) Deve ser feita a retenção da contribuição previdenciária no valor de 11% (onze por cento) sobre o valor da fatura e dos impostos incidentes sobre a prestação do serviço;

b) Deve ser consultada a situação da empresa junto ao SICAF;

c) Serão Exigidos a Certidão Negativa de Débitos (CND), relativa a Créditos Federais e à Dívida Ativa da União, o Certificado de Regularidade do FGTS (CRF) e a Certidão Negativa de Débitos Trabalhistas (CNDT), caso esses documentos não estejam regularizados no SICAF;

d) Deverá ser exigida, quando couber, comprovação de que a empresa mantém reserva de cargos para pessoa com deficiência ou para reabilitado da Previdência Social, conforme disposto no art. 66-A da Lei nº 8.666, de 1993. 16.17.

19.16. Fiscalização diária:

a) Devem ser evitadas ordens diretas do CFC dirigidas aos terceirizados. As solicitações de serviços devem ser dirigidas ao preposto da empresa. Da mesma forma, eventuais reclamações ou cobranças relacionadas aos empregados terceirizados devem ser dirigidas ao preposto.

b) Toda e qualquer alteração na forma de prestação do serviço, como a negociação de folgas ou a compensação de jornada, deve ser evitada, uma vez que essa conduta é exclusiva da contratada.

c) Devem ser conferidos, por amostragem, diariamente, os empregados terceirizados que estão prestando serviços e em quais funções, e se estão cumprindo a jornada de trabalho.

19.17. Cabe, ainda, à fiscalização do contrato, verificar se a Contratada observa a legislação relativa à concessão de férias e licenças aos empregados, respeita a estabilidade provisória de seus empregados e observa a data-base da categoria prevista na CCT, concedendo os reajustes dos empregados no dia e percentual previstos.

19.17.1. O gestor do contrato deverá verificar a necessidade de se proceder a repactuação do contrato, inclusive quanto à necessidade de solicitação da Contratada.

19.18. O CFC deverá solicitar, por amostragem, aos empregados, seus extratos da conta do FGTS e que verifiquem se as contribuições previdenciárias e do FGTS estão sendo recolhidas em seus nomes.

19.18.1. Ao final de um ano, todos os empregados devem ter seus extratos avaliados.

19.19. A Contratada deverá entregar, no prazo de 15 (quinze) dias, quando solicitado pelo CFC quaisquer dos seguintes documentos:

a) extrato da conta do INSS e do FGTS de qualquer empregado, a critério do CFC;

b) cópia da folha de pagamento analítica de qualquer mês da prestação dos serviços, em que conste como tomador o CFC;

c) cópia dos contracheques assinados dos empregados relativos a qualquer mês da prestação dos serviços ou, ainda, quando necessário, cópia de recibos de depósitos bancários; e

d) comprovantes de entrega de benefícios suplementares (vale-transporte, vale-alimentação, entre outros), a que estiver obrigada por força de lei, Acordo, Convenção ou Dissídio Coletivo de Trabalho, relativos a qualquer mês da prestação dos serviços e de qualquer empregado.

19.20. A fiscalização técnica dos contratos avaliará constantemente a execução do objeto e utilizará o Instrumento de Medição de Resultado (IMR), conforme modelo previsto no Anexo II, ou outro instrumento substituto para aferição da qualidade da prestação dos serviços, devendo haver o redimensionamento no pagamento com base nos indicadores estabelecidos, sempre que a Contratada:

a) não produzir os resultados, deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou

b) deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

19.20.1. A utilização do IMR não impede a aplicação concomitante de outros mecanismos para a avaliação da prestação dos serviços.

19.21. Durante a execução do objeto, o fiscal técnico deverá monitorar constantemente o nível de qualidade dos serviços para evitar a sua degeneração, devendo intervir para requerer à Contratada a correção das faltas, falhas e irregularidades constatadas.

19.22. O fiscal técnico deverá apresentar ao preposto da Contratada a avaliação da execução do objeto ou, se for o caso, a avaliação de desempenho e qualidade da prestação dos serviços realizada.

19.23. Em hipótese alguma, será admitido que a própria Contratada materialize a avaliação de desempenho e qualidade da prestação dos serviços realizada.

19.24. A Contratada poderá apresentar justificativa para a prestação do serviço com menor nível de conformidade, que poderá ser aceita pelo fiscal técnico, desde que comprovada a excepcionalidade da ocorrência, resultante exclusivamente de fatores imprevisíveis e alheios ao controle do prestador.

19.25. Na hipótese de comportamento contínuo de desconformidade da prestação do serviço em relação à qualidade exigida, bem como quando esta ultrapassar os níveis mínimos toleráveis previstos nos indicadores, além dos fatores redutores, devem ser aplicadas as sanções à Contratada de acordo com as regras previstas no ato convocatório.

19.26. O fiscal técnico poderá realizar avaliação diária, semanal ou mensal, desde que o período escolhido seja suficiente para avaliar ou, se for o caso, aferir o desempenho e qualidade da prestação dos serviços.

19.27. O representante da Contratante deverá ter a qualificação necessária para o acompanhamento e controle da execução dos serviços e do contrato.

19.28. A verificação da adequação da prestação do serviço deverá ser realizada com base nos critérios previstos neste Termo de Referência.

19.29. A fiscalização do contrato, ao verificar que houve subdimensionamento da produtividade pactuada, sem perda da qualidade na execução do serviço, deverá comunicar à autoridade responsável para que esta promova a adequação contratual à produtividade efetivamente realizada, respeitando-se os limites de alteração dos valores contratuais previstos no § 1º do art. 65 da Lei nº 8.666, de 1993.

19.30. O representante do CFC deverá promover o registro das ocorrências verificadas, adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais, conforme o disposto nos §§ 1º e 2º do art. 67 da Lei nº 8.666, de 1993. 16.33. O descumprimento total ou parcial das obrigações e responsabilidades assumidas pela Contratada, incluindo o descumprimento das obrigações trabalhistas, não recolhimento das contribuições sociais, previdenciárias ou para com o FGTS ou a não manutenção das condições de habilitação, ensejará a aplicação de sanções administrativas, previstas no instrumento convocatório e na legislação vigente, podendo culminar em rescisão contratual, por ato unilateral e escrito do CFC, conforme disposto nos arts. 77 e 80 da Lei nº 8.666, de 1993. 16.34. Caso não seja apresentada a documentação comprobatória do cumprimento das obrigações trabalhistas, previdenciárias e para com o FGTS, o CFC comunicará o fato à Contratada e reterá o pagamento da fatura mensal, em valor proporcional ao inadimplemento, até que a situação seja regularizada.

19.30.1. Não havendo quitação das obrigações por parte da Contratada no prazo de 15 (quinze) dias, o CFC poderá efetuar o pagamento das obrigações diretamente aos empregados da Contratada que tenham participado da execução dos serviços objeto do contrato.

19.30.2. O sindicato representante da categoria do trabalhador deverá ser notificado pelo CFC para acompanhar o pagamento das verbas mencionadas.

19.30.3. Tais pagamentos não configuram vínculo empregatício ou implicam a assunção de responsabilidade por quaisquer obrigações dele decorrentes entre a Contratante e os empregados da Contratada.

19.31. O contrato só será considerado integralmente cumprido após a comprovação, pela Contratada, do pagamento de todas as obrigações trabalhistas, sociais e previdenciárias e para com o FGTS referentes à mão de obra alocada em sua execução, inclusive quanto às verbas rescisórias.

19.32. A fiscalização de que trata este tópico não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade da Contratante ou de seus agentes, gestores e fiscais, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

19.33. As disposições previstas neste Termo de Referência não excluem o disposto no Anexo VIII da Instrução Normativa SLTI/MP nº 05, de 2017, aplicável no que for pertinente à contratação.

20. RECEBIMENTO E ACEITAÇÃO DO OBJETO

20.1. A emissão da Nota Fiscal/Fatura deve ser precedida do recebimento definitivo dos serviços, nos termos a seguir.

20.1.1. No prazo de até 5 (cinco) dias corridos do adimplemento da parcela, a Contratada deverá entregar toda a documentação comprobatória do cumprimento da obrigação contratual

20.1.2. O recebimento provisório será realizado pela equipe de fiscalização técnica e administrativa após a entrega da documentação acima, da seguinte forma:

20.1.2.1. A Contratante realizará inspeção dos serviços executados, por meio de profissionais técnicos competentes, com a finalidade de verificar a adequação dos serviços e constatar e relacionar os arremates, retoques e revisões finais que se fizerem necessários.

20.1.2.2. Para efeito de recebimento provisório, ao final de cada período mensal, o fiscal técnico do contrato deverá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos no ato convocatório, que poderá resultar no redimensionamento de valores a serem pagos à Contratada, registrando em relatório a ser encaminhado ao gestor do contrato.

20.1.2.3. A Contratada fica obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

20.1.2.4. Ao final de cada período de faturamento mensal, o fiscal administrativo deverá verificar as rotinas previstas no Anexo VIII-B da IN SEGES/MP nº 5/2017, no que forem aplicáveis à presente contratação, emitindo relatório que será encaminhado ao gestor do contrato.

20.1.3. No prazo de até 10 (dez) dias corridos a partir do recebimento dos documentos da Contratada, cada fiscal ou a equipe de fiscalização deverá elaborar Relatório Circunstanciado em consonância com suas atribuições, e encaminhá-lo ao gestor do contrato.

20.1.3.1. Quando a fiscalização for exercida por um único empregado, o relatório circunstanciado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

20.1.3.2. Será considerado como ocorrido o recebimento provisório com a entrega do relatório circunstanciado ou, em havendo mais de um a ser feito, com a entrega do útil.

19.3.2.2.1 Na hipótese de a verificação a que se refere o parágrafo anterior não ser procedida tempestivamente, reputar-se-á como realizada, consumando-se o recebimento provisório no dia do esgotamento do prazo.

20.1.4. No prazo de até 5 (cinco) dias corridos a partir do recebimento provisório dos serviços, o Gestor do Contrato deverá providenciar o recebimento definitivo, ato que concretiza o ateste da execução dos serviços, obedecendo as seguintes diretrizes:

20.1.4.1. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à Contratada, por escrito, as respectivas correções;

20.1.4.2. Emitir Termo Circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e

20.1.4.3. Comunicar à empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização, com base no Instrumento de Medição de Resultado (IMR), ou instrumento substituto.

20.1.5. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da Contratada pelos prejuízos resultantes da incorreta execução do contrato, ou, em qualquer época, das garantias concedidas e das responsabilidades assumidas em contrato e por força das disposições legais em vigor (Lei nº 10.406, de 2002).

20.1.6. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser corrigidos/refeitos/substituídos no prazo fixado pelo fiscal do contrato, às custas da Contratada, sem prejuízo da aplicação de penalidades.

21. PAGAMENTO

21.1. O pagamento da obrigação deverá ocorrer no prazo previsto no contrato, limitado:

- a) ao quinto dia útil subsequente ao recebimento da Nota Fiscal ou Fatura para despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei nº 8.666, de 1993, observado o disposto no seu § 1º; ou
- b) a trinta dias contados do recebimento da Nota Fiscal ou Fatura, para os demais casos.

21.2. Considera-se ocorrido o recebimento da Nota Fiscal ou Fatura no momento em que o órgão contratante atestar a execução do objeto do contrato.

21.3. A emissão da Nota Fiscal/Fatura será precedida do recebimento provisório e definitivo do serviço, nos seguintes termos:

21.3.1. A emissão do Termo Circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e

21.3.2. A comunicação a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

21.4. O pagamento somente será autorizado depois de efetuado o “atesto” pelo empregado competente, devidamente acompanhado das comprovações mencionadas no item 2 do Anexo XI da IN SEGES/MPDG nº 05/2017.

21.5. Caso se constate o descumprimento de obrigações trabalhistas ou da manutenção das condições exigidas para habilitação poderá ser concedido um prazo para que a Contratada regularize suas obrigações, quando não se identificar má-fé ou a incapacidade de corrigir a situação.

21.6. Não sendo regularizada a situação da Contratada no prazo concedido, ou nos casos em que identificada má-fé, se não for possível a realização desses pagamentos pela própria Administração, os valores retidos cautelarmente serão depositados junto à Justiça do Trabalho, com o objetivo de serem utilizados exclusivamente no pagamento de salários e das demais verbas trabalhistas, bem como das contribuições sociais e FGTS decorrentes.

21.7. Será considerada data do pagamento, o dia em que constar como emitida a ordem bancária para pagamento.

21.8. Antes de cada pagamento à Contratada, será realizada consulta para verificar a manutenção das condições de habilitação exigidas no edital.

21.9. Constatando-se a situação de irregularidade da contratada, será providenciada sua advertência, por escrito, para que, no prazo de 5 (cinco) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante.

21.10. Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

21.11. Persistindo a irregularidade, a Contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à Contratada a ampla defesa.

21.12. Para efeito do pagamento o CFC irá observar:

21.12.1. As faltas ao serviço do pessoal designado para execução dos serviços, conforme apontado pelo Fiscal do Contrato, desde que não tenham sido promovidas as devidas substituições, sem prejuízo da aplicação de penalidades, devendo deduzir o valor correspondente do valor da Nota Fiscal/Fatura.

- 21.12.2. O cumprimento das obrigações trabalhistas e sociais;
- 21.12.3. Recolhimento da contribuição previdenciária estabelecida para o empregador e de seus empregados, conforme dispõe o artigo 195, § 3º da Constituição Federal, sob pena de rescisão contratual;
- 21.12.4. Recolhimento do FGTS, referente ao mês anterior;
- 21.12.5. Pagamento de salários no prazo previsto em Lei, referente ao mês anterior da prestação dos serviços;
- 21.12.6. Fornecimento de Vale-Transporte e Auxílio-Alimentação, quando cabível, referente ao mês subsequente;
- 21.12.7. Pagamento do 13º salário;
- 21.12.8. Concessão de férias e correspondente pagamento do adicional de férias, na forma da Lei;
- 21.12.9. Realização de exames admissionais e demissionais e periódicos, quando for o caso;
- 21.12.10. Eventuais cursos de treinamento e reciclagem;
- 21.12.11. Encaminhamento das informações trabalhistas exigidas pela legislação, tais como RAIS e a CAGED;
- 21.12.12. Cumprimento das obrigações contidas em convenção coletiva, acordo coletivo ou sentença normativa em dissídio coletivo de trabalho;
- 21.12.13. Cumprimento das demais obrigações dispostas na CLT em relação aos empregados vinculados ao contrato;
- 21.12.14. Espelho da folha de pagamento específica do contrato;
- 21.12.15. Cópia da Relação dos Trabalhadores Constantes do Arquivo SEFIP (RE);
- 21.12.16. Os recolhimentos das contribuições ao INSS;
- 21.12.17. Cópia do Protocolo de Envio de Arquivos, emitido pela Conectividade Social (GFIP);
- 21.12.18. Cópia do Comprovante de Declaração à Previdência;
- 21.12.19. Examinar as Carteiras Profissionais dos empregados colocados a seu serviço, para comprovar o registro de função profissional.
- 21.12.20. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a Contratada não regularize sua situação junto ao SICAF.
- 21.13. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável, nos termos do item 6 do Anexo XI da IN SEGES/MPDG nº 05/2017, quando couber.
- 21.14. A Contratada regularmente optante pelo Simples Nacional, exclusivamente para as atividades de prestação de serviços previstas no §5º-C, do art. 18, da LC nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime, observando-se as exceções nele previstas. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário previsto na referida Lei Complementar.
- 21.15. Caso o pagamento não seja efetuado de acordo com o prazo estabelecido neste Termo de Referência, serão devidos à Contratada juros de mora de 0,03% (três centésimos por cento) ao dia, referente ao período compreendido entre a data do vencimento do prazo para pagamento até a data de sua efetivação.
- 21.16. O CFC reserva-se o direito de não efetivar o pagamento se, no ato da atestação pelo executor do contrato, caso os serviços não estiverem sendo prestados de acordo com o proposto, aceito e contratado.
- 21.17. O CFC efetuará a retenção dos encargos trabalhistas:
- 21.17.1. Os encargos trabalhistas relativos a férias, 13º salário e multa do FGTS por dispensa sem justa causa, a serem pagas pela Contratante à Contratada serão glosadas do valor mensal do contrato e depositadas exclusivamente em banco oficial público:
- I) Os depósitos de que trata o *caput* deste subitem devem ser efetivados em conta corrente vinculada – bloqueada para movimentação – aberta em nome da empresa, unicamente para essa finalidade e com movimentação somente por ordem do CFC;
- II) A solicitação de abertura e a autorização para movimentar a conta corrente vinculada – bloqueada para movimentação – serão providenciadas pelo CFC;
- III) Os depósitos serão efetuados com o acréscimo do Lucro proposto pela Contratada.
- 21.17.2. O montante do depósito vinculado será igual ao somatório dos valores das seguintes provisões previstas para o período de contratação:
- I) 13º salário;
- II) Férias e Abono de Férias;
- III) Impacto sobre férias e 13º salário;
- IV) Multa do FGTS.
- 21.17.3. Os valores provisionados para o atendimento do que trata o item anterior serão obtidos pela aplicação de percentuais e valores constantes da proposta;
- 21.18. O eventual atraso na entrega da Nota Fiscal acarretará correspondente e proporcional atraso no pagamento, sem qualquer penalização ou atualização monetária.
- 21.19. O documento de cobrança será emitido em nome do Conselho Federal de Contabilidade, sem emendas ou rasuras, fazendo menção expressa ao número da Licitação e contendo todos os seus dados e outros conforme abaixo especificado:

21.20. O número de inscrição no CNPJ da empresa deverá ser o mesmo da documentação apresentada para habilitação, da Proposta Comercial e do documento de cobrança. Na hipótese de divergência entre o CNPJ constante do contrato e do documento de cobrança, deverá a fornecedora apresentar Declaração (juntamente com este último documento), justificando este procedimento e, ao mesmo tempo, se responsabilizando pela regularidade fiscal do estabelecimento comercial emitente do documento de cobrança.

21.21. De acordo com o artigo 64 da Lei nº 9.430, de 27.12.96, os pagamentos efetuados por Órgãos, Autarquias e Fundações da Administração Pública Federal a Pessoas Jurídicas, pelo fornecimento de bens e/ou prestação de serviços, estão sujeitos à incidência na fonte, do Imposto sobre a Renda, da Contribuição Social sobre o Lucro Líquido, da Contribuição para Seguridade Social – Cofins e da Contribuição para Pis/Pasep.

21.22. A tabela de bens e serviços a que se refere o item anterior está à disposição de todos os interessados no site da Receita Federal: www.receita.fazenda.gov.br, (IN SRF nº 1.234 de 11 de janeiro de 2012 com alterações dada pela IN SRF nº 1.540 de 5 de janeiro de 2015) e por ocasião do pagamento, conforme o caso, todos os impostos serão retidos na fonte conforme a legislação vigente.

21.23. Caso a Contratada seja optante pelo “SIMPLES” a cada fornecimento e a cada emissão de Nota Fiscal, deverá juntar a declaração ORIGINAL de isenção dos impostos, em 02 (duas) vias, assinada com identificação do assinante e nome da empresa.

21.24. O documento de cobrança (Nota Fiscal) deverá ser formulado, já constando todos os impostos e/ou tributos incidentes que serão retidos conforme IN SRF nº 1234 de 11 de janeiro de 2012 com alterações dada pela IN SRF nº 1.540 de 5 de janeiro de 2015, sob pena de devolução para correção, contando-se o prazo para o pagamento a partir do recebimento regular da mesma.

21.25. Optando pelo depósito bancário, no documento de cobrança deverá constar o nome e o número do banco, bem como o nome e o número da agência e o número da conta à qual se dará o depósito bancário para pagamento, repetindo-se os dados contidos na Proposta Comercial.

21.26. Qualquer alteração de dados bancários só será permitida desde que efetuada em papel timbrado da empresa, assinada por representante legal e encaminhada ao Departamento de Compras e Licitações, antes do processamento do respectivo pagamento.

21.27. Caso a Contratada deixe de atender, mesmo que de forma parcial, as regras contidas neste Termo de Referência, o pagamento ficará retido até seu pleno atendimento e não caracterizará, em hipótese alguma, inadimplência por parte do CFC.

22. CONTA VINCULADA

22.1. Para atendimento ao disposto no art. 18 da IN SEGES/MP N. 5/2017, as regras acerca da Conta-Depósito Vinculada a que se refere o Anexo XII da IN SEGES/MP n. 5/2017 são as estabelecidas neste Termo de Referência.

22.1.1. Será adotado mecanismo da Conta-Depósito Vinculada para otimizar e tornar mais eficiente o processo de controle da conta-depósito vinculada a ser executado pelo Fiscal Administrativo. A adoção desse procedimento é necessária tendo em vista que a alocação de pessoal do CFC é relativamente restrita para a realização dessa atividade e os funcionários designados estarem capacitados para esse processo. Caso a opção fosse pelo 'pagamento por fator gerador' a fiscalização teria uma demanda maior de trabalhos para conferência dos documentos relativos aos pagamentos das verbas trabalhistas (13º salário, férias e 1/3 constitucional, multa de FGTS) e de outros eventos incertos (dias pagos pela licença a paternidade, maternidade, dia para doar sangue).

22.2. A futura Contratada deve autorizar a Administração contratante, no momento da assinatura do contrato, a fazer o desconto nas faturas e realizar os pagamentos dos salários e demais verbas trabalhistas diretamente aos trabalhadores, bem como das contribuições previdenciárias e do FGTS, quando não demonstrado o cumprimento tempestivo e regular dessas obrigações, até o momento da regularização, sem prejuízo das sanções cabíveis.

22.3. Quando não for possível a realização desses pagamentos pela própria Administração (ex.: por falta da documentação pertinente, tais como folha de pagamento, rescisões dos contratos e guias de recolhimento), os valores retidos cautelarmente serão depositados junto à Justiça do Trabalho, com o objetivo de serem utilizados exclusivamente no pagamento de salários e das demais verbas trabalhistas, bem como das contribuições sociais e FGTS decorrentes.

22.4. A Contratada autorizará o provisionamento de valores para o pagamento das férias, 13º salário e rescisão contratual dos trabalhadores da contratada, bem como de suas repercussões trabalhistas, fundiárias e previdenciárias, que serão depositados pela Contratante em conta-depósito vinculada específica, em nome do prestador dos serviços, bloqueada para movimentação, conforme disposto no Anexo XII da Instrução Normativa SEGES/MP nº 5, de 2017, os quais somente serão liberados para o pagamento direto dessas verbas aos trabalhadores, nas condições estabelecidas no item 1.5 do anexo VII-B da referida norma.

22.5. O montante dos depósitos da conta vinculada, conforme item 2 do Anexo XII da IN SEGES/MP n. 5/2017 será igual ao somatório dos valores das provisões a seguir discriminadas, incidentes sobre a remuneração, cuja movimentação dependerá de autorização do órgão ou entidade promotora da licitação e será feita exclusivamente para o pagamento das respectivas obrigações:

22.5.1. 13º (décimo terceiro) salário;

22.5.2. Férias e um terço constitucional de férias;

22.5.3. Multa sobre o FGTS e contribuição social para as rescisões sem justa causa; e

22.5.4. Encargos sobre férias e 13º (décimo terceiro) salário.

22.5.5. Os percentuais de provisionamento e a forma de cálculo serão aqueles indicados no Anexo XII da IN SEGES/MP n. 5/2017. 19.5 O saldo da conta-depósito será remunerado pelo índice de correção da poupança *pro rata die*, conforme definido em Termo de Cooperação Técnica firmado entre o promotor desta licitação e instituição financeira. Eventual alteração da forma de correção implicará a revisão do Termo de Cooperação Técnica.

22.6. Os valores referentes às provisões mencionadas neste edital que sejam retidos por meio da conta-depósito deixarão de compor o valor mensal a ser pago diretamente à empresa que vier a prestar os serviços.

22.7. Em caso de cobrança de tarifa ou encargos bancários para operacionalização da conta-depósito, os recursos atinentes a

essas despesas serão debitados dos valores depositados.

22.8. A empresa contratada poderá solicitar a autorização do órgão ou entidade Contratante para utilizar os valores da conta-depósito para o pagamento dos encargos trabalhistas previstos nos subitem acima ou de eventuais indenizações trabalhistas aos empregados, decorrentes de situações ocorridas durante a vigência do contrato.

22.8.1. Na situação do subitem acima, a empresa deverá apresentar os documentos comprobatórios da ocorrência das obrigações trabalhistas e seus respectivos prazos de vencimento. Somente após a confirmação da ocorrência da situação pela Administração, será expedida a autorização para a movimentação dos recursos creditados na conta-depósito vinculada, que será encaminhada à Instituição Financeira no prazo máximo de 5 (cinco) dias úteis, a contar da data da apresentação dos documentos comprobatórios pela empresa.

22.8.2. A autorização de movimentação deverá especificar que se destina exclusivamente para o pagamento dos encargos trabalhistas ou de eventual indenização trabalhista aos trabalhadores favorecidos.

22.8.3. A empresa deverá apresentar ao órgão ou entidade contratante, no prazo máximo de 3 (três) dias úteis, contados da movimentação, o comprovante das transferências bancárias realizadas para a quitação das obrigações trabalhistas.

22.9. O saldo remanescente dos recursos depositados na conta-depósito será liberado à respectiva titular no momento do encerramento do contrato, na presença do sindicato da categoria correspondente aos serviços contratados, quando couber, e após a comprovação da quitação de todos os encargos trabalhistas e previdenciários relativos ao serviço contratado, conforme item 15 da IN SEGES/MP n. 5/2017.

22.10. Encaminhar Anexo IX Autorização Complementar ao Contrato.

23. REAJUSTE / REPACTUAÇÃO

23.1. **Para o Item 01 - Serviço de Suporte Técnico com Monitoramento de ativos 24x7 e Operação Remota (Centro de Operação Remoto)**

23.1.1. Os preços são fixos e irrealizáveis no prazo de um ano contado da data limite para a apresentação das propostas.

23.1.2. Dentro do prazo de vigência do contrato e mediante solicitação da contratada, os preços contratados poderão sofrer reajuste após o interregno de um ano, aplicando-se o índice de reajustamento ICTI (Índice de Custos de Tecnologia da Informação), mantido pela Fundação Instituto de Pesquisa Econômica Aplicada (IPEA) (art. 24, da IN/SGD nº 31/2021), exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade:

$R = V (I - I^0) / I^0$, onde:

R = Valor do reajuste procurado;

V = Valor contratual do serviço a ser reajustado;

I⁰ = índice inicial - refere-se ao índice de custos ou de preços correspondente à data fixada para entrega da proposta da licitação;

I = Índice relativo ao mês do reajustamento;

23.1.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

23.1.4. No caso de atraso ou não divulgação do índice de reajustamento, o CFC pagará à Contratada da a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo. Fica a Contratada obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.

23.1.5. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.

23.1.6. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.

23.1.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

23.1.8. O reajuste será realizado por apostilamento.

23.2. **Para o Item 02 - Prestação de serviços técnicos de Administração, Suporte e Operação de Rede de Dados Local**

23.2.1. Visando à adequação aos novos preços praticados no mercado, desde que solicitado pela Contratada e observado o interregno mínimo de 1 (um) ano contado na forma apresentada no subitem que se seguirá, o valor consignado no Termo de Contrato será repactuado, competindo à Contratada justificar e comprovar a variação dos custos, apresentando memória de cálculo e planilhas apropriadas para análise e posterior aprovação do CFC, na forma estatuída no Decreto nº 9.507, de 2018, e nas disposições aplicáveis da Instrução Normativa SEGES/MP nº 5, de 2017.

23.2.2. A repactuação poderá ser dividida em tantas parcelas quantas forem necessárias, em respeito ao princípio da anualidade do reajustamento dos preços da contratação, podendo ser realizada em momentos distintos para discutir a variação de custos que tenham sua anualidade resultante em datas diferenciadas, tais como os custos decorrentes da mão de obra e os custos decorrentes dos insumos necessários à execução do serviço.

23.2.3. O interregno mínimo de 1 (um) ano para a primeira repactuação será contado:

23.2.3.1. Para os custos relativos à mão de obra, vinculados à data-base da categoria profissional: a partir dos efeitos financeiros do acordo, dissídio ou convenção coletiva de trabalho, vigente à época da apresentação da proposta, relativo a cada categoria profissional abrangida pelo contrato;

23.2.3.2. Para os insumos discriminados na Planilha de Custos e Formação de Preços que estejam diretamente vinculados ao valor de preço público (tarifa): do último reajuste aprovado por autoridade governamental ou realizado por determinação legal ou normativa;

23.2.3.3. Para os demais custos, sujeitos à variação de preços do mercado (insumos não decorrentes da mão de obra): a partir da data limite para apresentação das propostas constante do Edital.

23.2.3.4. Dentro do prazo de vigência do contrato e mediante solicitação da contratada, os preços contratados poderão sofrer reajuste após o interregno de um ano, aplicando-se o índice de reajustamento ICTI (Índice de Custos de Tecnologia da Informação), mantido pela Fundação Instituto de Pesquisa Econômica Aplicada (IPEA) (art. 24, da IN 01/2019), exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade:

23.2.4. Nas repactuações subsequentes à primeira, o interregno de um ano será computado da última repactuação correspondente à mesma parcela objeto de nova solicitação. Entende-se como última repactuação, a data em que iniciados seus efeitos financeiros, independentemente daquela em que celebrada ou apostilada.

23.2.5. O prazo para a Contratada solicitar a repactuação encerra-se na data da prorrogação contratual subsequente ao novo acordo, dissídio ou convenção coletiva que fixar os novos custos de mão de obra da categoria profissional abrangida pelo contrato, ou na data do encerramento da vigência do contrato, caso não haja prorrogação.

23.2.6. Caso a Contratada não solicite a repactuação tempestivamente, dentro do prazo acima fixado, ocorrerá a preclusão do direito à repactuação.

23.2.7. Nessas condições, se a vigência do contrato ver sido prorrogada, nova repactuação só poderá ser pleiteada após o decurso de novo interregno mínimo de 1 (um) ano, contado:

- a) da vigência do acordo, dissídio ou convenção coletiva anterior, em relação aos custos decorrentes de mão de obra;
- b) do último reajuste aprovado por autoridade governamental ou realizado por determinação legal ou normativa, para os insumos discriminados na planilha de custos e formação de preços que estejam diretamente vinculados ao valor de preço público (tarifa);
- c) do dia em que se completou um ou mais anos da apresentação da proposta, em relação aos custos sujeitos à variação de preços do mercado.

23.2.8. Caso, na data da prorrogação contratual, ainda não tenha sido celebrado o novo acordo, dissídio ou convenção coletiva da categoria, ou ainda não tenha sido possível à Contratante ou à Contratada proceder aos cálculos devidos, deverá ser inserida cláusula no termo aditivo de prorrogação para resguardar o direito futuro à repactuação, a ser exercido tão logo se disponha dos valores reajustados, sob pena de preclusão.

23.2.9. Quando a contratação envolver mais de uma categoria profissional, com datas base diferenciadas, a repactuação deverá ser dividida em tantas parcelas quantos forem os acordos, dissídios ou convenções coletivas das categorias envolvidas na contratação.

23.2.10. É vedada a inclusão, por ocasião da repactuação, de benefícios não previstos na proposta inicial, exceto quando se tornarem obrigatórios por força de instrumento legal, sentença normativa, Acordo, Convenção e Dissídio Coletivo de Trabalho.

23.2.11. A Contratante não se vincula às disposições contidas em Acordos, Dissídios ou Convenções Coletivas que tratem do pagamento de participação dos trabalhadores nos lucros ou resultados da empresa contratada, de matéria não trabalhista, de obrigações e direitos que somente se aplicam aos contratos com a Administração Pública, ou que estabeleçam direitos não previstos em lei, tais como valores ou índices obrigatórios de encargos sociais ou previdenciários, bem como de preços para os insumos relacionados ao exercício da atividade.

23.2.12. Quando a repactuação se referir aos custos da mão de obra, a Contratada efetuará a comprovação da variação dos custos dos serviços por meio de Planilha de Custos e Formação de Preços, acompanhada da apresentação do novo acordo, dissídio ou convenção coletiva da categoria profissional abrangida pelo contrato.

23.2.13. Quando a repactuação se referir aos custos sujeitos à variação dos preços de mercado (insumos não decorrentes da mão de obra), a Contratada demonstrará o respectivo aumento por meio de Planilha de Custos e Formação de Preços, considerando-se a aplicação do índice de reajustamento ICTI (Índice de Custos de Tecnologia da Informação), mantido pela Fundação Instituto de Pesquisa Econômica Aplicada (IPEA) (art. 24, da IN 01/2019), exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade, mediante a aplicação da seguinte fórmula (art. 5º do Decreto n.º 1.054, de 1994):

$R = V (I - I^0) / I^0$, onde:

R = Valor do reajuste procurado;

V = Valor contratual do serviço a ser reajustado;

I^0 = índice inicial - refere-se ao índice de custos ou de preços correspondente à data fixada para entrega da proposta da licitação;

I = Índice relativo ao mês do reajustamento;

23.2.13.1. No caso de atraso ou não divulgação do índice de reajustamento, o CFC pagará à Contratada a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo; fica a Contratada obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.

23.2.13.2. Nas aferições finais, o índice utilizado para a repactuação dos insumos será, obrigatoriamente, o definitivo.

23.2.13.3. Caso o índice estabelecido para a repactuação de insumos venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.

23.2.13.4. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente dos insumos e materiais, por meio de termo aditivo.

23.2.14. Os novos valores contratuais decorrentes das repactuações terão suas vigências iniciadas observando-se o seguinte:

23.2.14.1. a partir da ocorrência do fato gerador que deu causa à repactuação;

23.2.14.2. em data futura, desde que acordada entre as partes, sem prejuízo da contagem de periodicidade para concessão das próximas repactuações futuras; ou

23.2.14.3. em data anterior à ocorrência do fato gerador, exclusivamente quando a repactuação envolver revisão do custo de mão de obra em que o próprio fato gerador, na forma de acordo, dissídio ou convenção coletiva, ou sentença normativa, contemplar data de vigência retroativa, podendo esta ser considerada para efeito de compensação do pagamento devido, assim como para a contagem da anualidade em repactuações futuras.

23.2.15. Os efeitos financeiros da repactuação ficarão restritos exclusivamente aos itens que a motivaram, e apenas em relação à diferença porventura existente.

23.2.16. A decisão sobre o pedido de repactuação deve ser feita no prazo máximo de sessenta dias, contados a partir da solicitação e da entrega dos comprovantes de variação dos custos.

23.2.17. O prazo referido no subitem anterior ficará suspenso enquanto a Contratada não cumprir os atos ou apresentar a documentação solicitada pela Contratante para a comprovação da variação dos custos.

23.2.18. As repactuações serão formalizadas por meio de apostilamento, exceto quando coincidirem com a prorrogação contratual, caso em que deverão ser formalizadas por aditamento ao contrato.

23.2.19. A Contratada deverá complementar a garantia contratual anteriormente prestada, de modo que se mantenha a proporção de 5% (cinco por cento) em relação ao valor contratado, como condição para a repactuação, nos termos da alínea K do item 3.1 do Anexo VII-F da IN SEGES/MP n. 5/2017.

24. GARANTIA DA EXECUÇÃO

24.1. O adjudicatário prestará garantia de execução do contrato, nos moldes do art. 56 da Lei nº 8.666, de 1993, com validade durante a execução do contrato e por 90 (noventa) dias após o término da vigência contratual, em valor correspondente a 5% (cinco por cento) do valor total do contrato.

24.2. No prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do Contratante, contados da assinatura do contrato, a Contratada deverá apresentar comprovante de prestação de garantia, podendo optar por caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária.

24.2.1. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor total do contrato por dia de atraso, até o máximo de 2% (dois por cento).

24.2.2. O atraso superior a 25 (vinte e cinco) dias autoriza o CFC a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os incisos I e II do art. 78 da Lei n. 8.666 de 1993.

24.3. A validade da garantia, qualquer que seja a modalidade escolhida, deverá abranger um período de 90 (noventa) dias após o término da vigência contratual, conforme item 3.1 do Anexo VII-F da IN SEGES/MP nº 5/2017.

24.4. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

- a) prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;
- b) prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a execução do contrato;
- c) multas moratórias e punitivas aplicadas pela Administração à contratada; e
- d) obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pela Contratada, quando couber.

24.5. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item anterior, observada a legislação que rege a matéria.

24.6. A garantia em dinheiro deverá ser efetuada em favor da Contratante, em conta específica na Caixa Econômica Federal, com correção monetária.

24.7. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Economia.

24.8. No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

24.9. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada à nova situação ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.

24.10. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a Contratada obriga-se a fazer a respectiva reposição no prazo máximo de 10 (dez) dias úteis, contados da data em que for notificada.

24.11. A Contratante executará a garantia na forma prevista na legislação que rege a matéria.

24.12. Será considerada extinta a garantia:

- a) com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da Contratante, mediante termo circunstanciado, de que a Contratada cumpriu todas as cláusulas do contrato;
- b) no prazo de 90 (noventa) dias após o término da vigência do contrato, caso a Administração não comunique a ocorrência de sinistros, quando o prazo será ampliado, nos termos da comunicação, conforme estabelecido na alínea

"h2" do item 3.1 do Anexo VII-F da IN SEGES/MP n. 05/2017.

24.13. O garantidor não é parte para figurar em processo administrativo instaurado pela contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à Contratada.

24.14. A Contratada autoriza a contratante a reter, a qualquer tempo, a garantia, na forma prevista neste Termo de Referência.

24.15. A garantia da contratação somente será liberada ante a comprovação de que a empresa pagou todas as verbas rescisórias decorrentes da contratação, e que, caso esse pagamento não ocorra até o fim do segundo mês após o encerramento da vigência contratual, a garantia será utilizada para o pagamento dessas verbas trabalhistas, incluindo suas repercussões previdenciárias e relativas ao FGTS, conforme estabelecido no art. 8º, VI do Decreto nº 9.507, de 2018, observada a legislação que rege a matéria.

24.16. Também poderá haver liberação da garantia se a empresa comprovar que os empregados serão realocados em outra atividade de prestação de serviços, sem que ocorra a interrupção do contrato de trabalho

24.17. Por ocasião do encerramento da prestação dos serviços contratados, o CFC poderá utilizar o valor da garantia prestada para o pagamento direto aos trabalhadores vinculados ao contrato no caso da não comprovação:

a) do pagamento das respectivas verbas rescisórias; ou

b) da realocação dos trabalhadores em outra atividade de prestação de serviços, nos termos da alínea "j" do item 3.1 do Anexo VII-F da IN SEGES/MP n. 5/2017.

25. TRANSFERÊNCIA DE CONHECIMENTO E TRANSIÇÃO CONTRATUAL

25.1. A transferência de conhecimento, no uso das soluções desenvolvidas e implantadas pela Contratada, deverá ser viabilizada, sem ônus adicionais para a Contratante, com documentação clara e completa explicitando a metodologia utilizada.

25.2. Esta deverá ser direcionada para os técnicos indicados pela Contratante e focada na solução adotada. Ao final da transferência, os técnicos da Contratante deverão estar aptos e capacitados a realizarem a instalação, a manutenção, o monitoramento e a atualização do ambiente de Infraestrutura do Contratante.

25.3. Em ocorrendo nova licitação, com mudança de fornecedor dos serviços, a Contratada signatária do contrato em fase de expiração, assim considerado o período dos últimos três meses de vigência, deverá repassar para a vencedora do novo certame, por intermédio de evento formal, os documentos necessários à continuidade da prestação dos serviços, bem como esclarecer dúvidas a respeito de procedimentos no relacionamento entre a Contratante e a Contratada que se refiram ao Contratante.

26. VIGÊNCIA CONTRATUAL

26.1. O contrato decorrente do processo licitatório terá a vigência de 12 (doze) meses, contados a partir da data de sua assinatura, podendo este prazo ser prorrogado por períodos iguais e sucessivos, mediante Termo Aditivo, até o limite máximo de 60 (sessenta) meses, a partir da data de vigência do contrato, após a verificação da sua real necessidade e da vantajosidade para a Administração na sua continuidade, nos termos do inciso II do art. 57 da Lei no 8.666/93.

27. CRITÉRIO PARA ACEITABILIDADE DE PREÇOS

27.1. O critério de aceitabilidade de preço será:

27.1.1. Grupo 1 - Item 1 - valor unitário máximo aceitável: R\$328.440,00 (trezentos e vinte e oito mil quatrocentos e quarenta reais);

27.1.2. Grupo 1 - Item 2 - valor unitário máximo aceitável: R\$688.138,56 (seiscentos e oitenta e oito mil cento e trinta e oito reais e cinquenta e seis centavos).

27.1.3. A remuneração mínima aceitável para pagamento do profissional que ocupar o posto de trabalho "Analista de TI", a qual a CONTRATADA fica obrigada a cumprir, é de R\$ 8.750,00 (oito mil setecentos e cinquenta reais), conforme fundamentação constante no item 16 do Estudo Técnico Preliminar.

27.1.4. O patamar salarial mínimo previsto no item anterior será reajustado nos mesmos termos que os salários dos trabalhadores da categoria previstos em Convenção Coletiva de Trabalho.

27.1.5. - Caso a licitante apresente proposta constando remuneração do profissional abaixo do mínimo estabelecido no item 27.1.3, a proposta será presumida desclassificada, salvo se a licitante de forma fundamentada comprove a viabilidade dessa remuneração e essa fundamentação seja acatada pelo CFC.

27.1.6. Item da planilha de custos ANEXO VI - PLANILHA DE FORMAÇÃO DE CUSTOS, MÓDULO 6 – CUSTOS INDIRETOS, TRIBUTOS E LUCRO:

- A - Custos Indiretos e B - Lucro, o valor unitário máximo **somado** aceitável: 16 % (dezesesseis reais por cento).

27.2. O critério de julgamento da proposta é o menor preço GLOBAL para a seleção da proposta mais vantajosa, utilizado para compras e serviços de modo geral e para contratação de bens e serviços de informática.

27.3. A proposta deverá ser ofertada pelo VALOR GLOBAL DA PROPOSTA.

27.4. A proposta deverá ter validade de 90 (noventa) dias, contados da data da abertura do certame.

28. SANÇÕES ADMINISTRATIVAS

- 28.1. Comete infração administrativa nos termos da Lei nº 10.520, de 2002, a Contratada que:
- a) inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;
 - b) ensejar o retardamento da execução do objeto;
 - c) falhar ou fraudar na execução do contrato;
 - d) comportar-se de modo inidôneo; ou
 - e) cometer fraude fiscal.
- 28.2. Pela inexecução total ou parcial do objeto deste contrato, a Administração pode aplicar à Contratada as seguintes sanções:
- 28.2.1. Advertência por escrito, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado;
- 28.2.2. Multa de:
- a) 0,1% (um décimo por cento) até 0,2% (dois décimos por cento) por dia sobre o valor adjudicado em caso de atraso na execução dos serviços, limitada a incidência a 15 (quinze) dias. Após o décimo quinto dia e a critério da Administração, no caso de execução com atraso, poderá ocorrer a não-aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença;
 - b) 0,1% (um décimo por cento) até 10% (dez por cento) sobre o valor adjudicado, em caso de atraso na execução do objeto, por período superior ao previsto no subitem acima, ou de inexecução parcial da obrigação assumida;
 - c) 0,1% (um décimo por cento) até 15% (quinze por cento) sobre o valor adjudicado, em caso de inexecução total da obrigação assumida;
 - d) 0,2% a 3,2% por dia sobre o valor mensal do contrato, conforme detalhamento constante das tabelas 1 e 2, abaixo;
 - e) 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso na apresentação da garantia (seja para reforço ou por ocasião de prorrogação), observado o máximo de 2% (dois por cento). O atraso superior a 25 (vinte e cinco) dias autorizará o CFC a promover a rescisão do contrato;
 - f) 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso para o início da prestação dos serviços, observado o máximo de 2% (dois por cento). O atraso superior a 25 (vinte e cinco) dias autorizará o CFC a promover a rescisão do contrato.
- 28.2.2.1. As penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.
- 28.2.3. Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrava pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;
- 28.2.4. Sanção de impedimento de licitar e contratar com órgãos e entidades da União, com o consequente descredenciamento no SICAF pelo prazo de até cinco anos.
- 28.2.4.1. A Sanção de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipóteses previstas como infração administrava no subitem 28.1 deste Termo de Referência
- 28.2.5. Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados;
- 28.3. As sanções previstas nas alíneas a, c, d, e e f, do subitem 28.2.2 poderão ser aplicadas à CONTRATADA juntamente com as de multa, descontando-a dos pagamentos a serem efetuados.
- 28.4. Para efeito de aplicação de multas, às infrações são atribuídos graus, de acordo com as tabelas 1 e 2:

TABELA 1

GRAU	CORRESPONDÊNCIA
1	0,4% sobre o valor mensal do contrato
2	0,6% sobre o valor mensal do contrato
3	0,8% sobre o valor mensal do contrato
4	1,6% sobre o valor mensal do contrato
5	3,2% sobre o valor mensal do contrato

TABELA 2

INFRAÇÃO		
ITEM	DESCRIÇÃO	GRAU
1	Permitir situação que crie a possibilidade de causar dano físico, lesão corporal ou conseqüências letais. Por ocorrência	5
2	Retirar empregados, supervisor ou encarregado do serviço durante o expediente, sem a anuência prévia do CFC. Por ocorrência	1
3	Deixar de registrar e controlar, diariamente, a assiduidade e a pontualidade de seu pessoal	3
4	Deixar de substituir empregado que se conduza de modo inconveniente ou não atenda às necessidades do serviço. Por empregado e por dia	1
5	Deixar de indicar e manter durante a execução do contrato o preposto previsto no edital/contrato	3
6	Deixar de fornecer crachás ou atrasar no seu fornecimento. Por ocorrência	1
7	Deixar de substituir empregado que se apresentar sem crachá ou desatento às normas de higiene pessoal. Por ocorrência.	1
8	Deixar de apresentar registro de frequência de seus empregados, quando solicitado pelo fiscal do contrato. Por ocorrência	1
9	Deixar de fornecer a relação nominal dos empregados em serviço no CFC. Por ocorrência	2
10	Deixar de observar as determinações do CFC quanto a permanência e circulação de seus empregados no prédio em horário e dia não autorizados. Por ocorrência	1
11	Deixar de comunicar, por escrito, ao CFC imediatamente após o fato, qualquer anormalidade ocorrida nos serviços. Por ocorrência.	1
12	Deixar de cumprir as exigências relativas à medicina e segurança do trabalho. Por ocorrência.	4
13	Deixar de manter, em serviço, número de empregados efetivamente contratados. Por ocorrência.	5
14	Deixar de pagar em dia os salários ou acréscimos salariais decorrentes de lei, contrato ou dissídio. Por empregado e por dia	1
15	Deixar de fornecer auxílio transporte ou auxílio alimentação a seus empregados. Por empregado e por dia.	1
16	Deixar de orientar os seus empregados quanto a adoção do Plano de Logística Sustentável do CFC e das Normas de Segurança. Por ocorrência	4
17	Deixar de substituir empregado em caso de eventual ausência, tais como faltas, férias, atrasos e licenças. Por ocorrência e por dia.	1
18	Deixar de fornecer, sempre que solicitados pela Contratante, os comprovantes do cumprimento das obrigações previdenciárias, do Fundo de Garantia do Tempo de Serviço (FGTS) e do pagamento dos salários e demais benefícios trabalhistas dos empregados colocados à disposição da Contratante. Por ocorrência	1
19	Deixar de comunicar ao Fiscal do Contrato, no prazo máximo de 24 (vinte e quatro) horas, o desligamento de empregado da contratada. Por ocorrência.	1

20	Deixar de fornecer ao Fiscal do contrato relatório constando relações nominais de licenças, faltas, se houver, bem como escala nominal de férias dos empregados. Por ocorrência.	1
21	Deixar de recolher em dia as contribuições sociais, previdenciárias e FGTS . Por dia.	3
22	Deixar de cumprir quaisquer dos itens do Edital e seus Anexos não previstos nesta tabela de multas, após reincidência formalmente notificada pelo CFC, por ocorrência.	3
23	Deixar de cumprir com as obrigações trabalhistas e previdenciárias. Por ocorrência da inadimplência e por mês.	5

28.5. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

28.5.1. tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

28.5.2. tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

28.5.3. demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

28.6. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

28.7. As multas devidas e/ou prejuízos causados à Contratante serão deduzidos dos valores a serem pagos, ou recolhidos em favor da Contratante, ou deduzidos da garantia, ou ainda, quando for o caso, serão inscritos na Dívida Ativa da União e cobrados judicialmente.

28.7.1. Caso a Contratante determine, a multa deverá ser recolhida no prazo máximo de 15 (quinze) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

28.8. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

29. CRITÉRIOS DE SUSTENTABILIDADE AMBIENTAL

29.1. A Contratada deverá adotar práticas de sustentabilidade ambiental na execução do objeto, quando couber, conforme disposto na Instrução Normativa nº 1/2010 - SLTI/MPOG.

30. ESTIMATIVA DE PREÇOS OU PREÇOS REFERENCIAIS

30.1. O custo estimado da contratação é de R\$1.016.578,56 (um milhão, dezesseis mil quinhentos e setenta e oito reais e cinquenta e seis centavos).

31. DOTAÇÃO ORÇAMENTÁRIA

31.1. A conexão entre contratação e o planejamento existente está contido no Projeto 5002 – Tecnologia da Informação, constante no Plano de Trabalho do CFC. A despesa decorrente do contrato ocorrerá nas conta contábil 6.3.1.3.02.01.005 – Serviços de Tecnologia da Informação.

32. ANEXOS

32.1. ANEXO I – Especificações técnicas dos serviços.

32.2. ANEXO II – Instrumento de Medição de Resultado (IMR).

32.3. ANEXO III – Termo de confidencialidade e sigilo.

32.4. ANEXO IV - Termo de Ciência.

32.5. ANEXO V – Modelo de apresentação de proposta de preços.

32.6. ANEXO VI – Modelo de planilha de custos e formação de preços (doc. SEI nº 0047472). (Externo)

32.7. ANEXO VII – Planilha de custos e formação de preços (doc. SEI nº 0044601) . (Externo)

32.8. ANEXO VIII – Comprovação técnica.

32.9. ANEXO IX - Autorização Complementar ao Contrato.

32.10. ANEXO X - Modelo de relação de compromissos assumidos.

EQUIPE DE PLANEJAMENTO**Rogério Ribeiro da Silva**

Gerente do Departamento de Informática
Assinatura via SEI.

Marcos Antonio Alves de Oliveira Pinto

Analista de Sistemas
Assinatura via SEI.

Gilson Luiz de Castro

Técnico em Contabilidade
Assinatura via SEI.

Conferido e de acordo.

A justificativa apresentada, especificações técnicas e quantitativas, contidas no presente instrumento, demonstram-se satisfatórias e suficientes para o atendimento às necessidades do CFC.

Andréa Rodrigues Rosa

Coordenadora de Gestão de TI
Assinatura via SEI

Aprovo o Termo de Referência.

Encaminhe-se ao Departamento de Licitações e Contratos para as providências necessárias.

Elys Tevania Alves de Souza Carvalho

Diretora Executiva
Assinatura via SEI

ANEXO I

ESPECIFICAÇÕES TÉCNICAS DOS SERVIÇOS

1. INTRODUÇÃO

1.1. A Tecnologia da Informação tem evoluído de maneira extremamente veloz e diversa para atender a constante demanda por competitividade, novas regulamentações, exigências legais, dentre outros. Conceitos como Cloud Computing e Virtualização são exemplos de novas abordagens tecnológicas que têm sido adotadas por todas as organizações em busca de sistemas de informação mais disponíveis, flexíveis e escaláveis.

1.2. O setor de Tecnologia da Informação do Conselho Federal de Contabilidade tem como princípio básico atender com qualidade e eficiência as demandas da organização, planejando e realizando os investimentos necessários nos sistemas de informação e infraestrutura de tecnologia que o suportam, a saber:

- a) Sistema de Correio Eletrônico;
- b) Portal CFC;
- c) Sistemas finalísticos de Registro, Fiscalização, Educação Profissional Continuada e sistemas internos diversos;
- d) Sistema de armazenamento, backup e servidores;
- e) Sistemas de Segurança da Informação;
- f) Redundância de informações, conforme exigências e regulamentações;

1.3. O aumento da dependência das organizações com relação aos seus sistemas de informação e o incremento do nível de complexidade para manter o ambiente de TI funcionando nos níveis de disponibilidade, desempenho e segurança exigidos, traz à tona a necessidade de definir e manter indicadores constantemente monitorados para os principais ativos de tecnologia da informação, permitindo a atuação preventiva nas atividades de suporte e manutenção dos componentes da rede.

1.4. Aplicações como os sistemas publicados na Internet, como sistemas finalísticos de registro, fiscalização, educação Continuada, correio eletrônico, site institucional do Conselho Federal de Contabilidade e seus banco de dados, dentre outros devem agora estar disponíveis em regime 24 horas x 7 dias por semana, para atender as necessidades do negócio da organização e seus clientes. Consequentemente, pessoal técnico especializado deveria estar disponível também em período integral (24 h x 7 d/s) para garantir os novos níveis de disponibilidade exigidos, o que não ocorre atualmente e seria financeiramente inviável implantar com o reduzido corpo técnico atual de tecnologia da informação do Conselho Federal de Contabilidade.

1.5. Diante do exposto, a contratação de serviços especializados, objetiva contribuir para o incremento dos níveis de disponibilidade, desempenho e segurança dos sistemas de informação da empresa e serviços por ela prestados.

2. OBJETO

2.1. O objeto desta licitação é a contratação de empresa especializada para prestação de serviços técnicos de Administração, Operação Remota, Monitoramento em Regime 24x7 do Ambiente de Tecnologia da Informação do Conselho Federal de Contabilidade (CFC) em Brasília – DF, bem como com posto fixo neste CFC, com pelo menos 2 (dois) funcionários para trabalhos no Regime de 5 dias x 8 horas diárias (horário de expediente do CFC), conforme especificação no Termo de Referência.

GRUPO	ITEM OU SERVIÇO	LOCAL DE EXECUÇÃO	HORÁRIO	PERÍODO	CARGA HORÁRIA
01	01	Serviço de Suporte Técnico com Monitoramento de ativos 24x7 e Operação Remota (Centro de Operação Remoto) Competências técnica item 5 do anexo I Especificações item 6 e 7 do anexo I	Serviço de Suporte e monitoramento de ativos: 24 x 7 Serviço de Operação Remoto: 16 x 5 dias úteis (fora do horário de expediente) e 24 x 2 dias não úteis)	Segunda à Domingo	Suporte e monitoramento: 168 horas Operação Remota 128 horas semanais
	02	Analista de TI para a prestação de serviços técnicos de Administração, Suporte e Operação de Rede de Dados Local Competências técnica item 4 do anexo I Especificações item 7 do anexo I	8 x 5 dias úteis (Segunda à Sexta) Horário de expediente do CFC	Segunda à Sexta	40 horas semanais

ATIVIDADE OU SERVIÇO	HORÁRIO	PERÍODO	CÓDIGO	OCUPAÇÃO
Serviços técnicos de suporte e Administração, suporte e operação de Rede de Dados Local	8 horas (horário de expediente do CFC)	Segunda a Sexta	2124-10	Analista de redes e de comunicação de dados

3. RESULTADOS E BENEFÍCIOS ESPERADOS

3.1. Entre os benefícios da adoção deste tipo de serviço, podemos destacar os seguintes:

- 3.1.1. Dispor de pessoal especializado e multidisciplinar para prestar os serviços de monitoramento e suporte técnico remoto, em regime 24 horas x 7 dias por semana;
- 3.1.2. Dispor de pessoal especializado e multidisciplinar para prestar os serviços de operação e administração, em regime de 16 x 5 (dias úteis) e 24 x 2 (dias não úteis) ;
- 3.1.3. Dispor de serviço de análise avançado de segurança, conforme especificações;
- 3.1.4. Dispor de 2 (dois) funcionários para trabalhos na área de Tecnologia da Informação do CFC, 8 horas diárias (horário de expediente do CFC) e 5 dias por semana. Poderá mediante autorização prévia do CFC, a realização de horas adicionais, nos limites definidos pelas Leis trabalhistas.
- 3.1.5. Redução do tempo do ciclo de vida das solicitações e incidentes de TI;
- 3.1.6. Diminuição da incidência de paralisações nos equipamentos de TI, planejando ações proativas para a redução de problemas, mantendo-se para isso equipe técnica qualificada, selecionada e acompanhada;
- 3.1.7. Atuação em áreas críticas utilizando-se de informações reais e práticas extraídas de relatórios estatísticos do software de acompanhamento e controle dos serviços de suporte;
- 3.1.8. Uniformidade no atendimento de equipamentos através de histórico das ocorrências e o aprendizado no combate a problemas;
- 3.1.9. Escalonamento mais rápido e eficiente dos incidentes e problemas junto ao suporte dos fabricantes das soluções de TI adotadas pelo Conselho Federal de Contabilidade;
- 3.1.10. Monitoramento de disponibilidade, desempenho e segurança de todo o parque de servidores, rede e aplicações;
- 3.1.11. Acompanhamento, atuação e efetivo aproveitamento dos contratos e prazos de garantia dos equipamentos junto aos fornecedores de equipamentos e serviços;
- 3.1.12. Desenvolvimento e manutenção de uma base de conhecimentos de TI;
- 3.1.13. Diminuição do tempo de parada da rede devido a problemas de infraestrutura de TI;
- 3.1.14. Maior segurança para as principais aplicações disponibilizadas pelo CFC.

4. COMPETÊNCIAS TÉCNICAS DOS ANALISTAS E PROFISSIONAIS QUE EXECUTARÃO OS SERVIÇOS

4.1. COMPETÊNCIAS TÉCNICAS EXIGIDAS DOS ANALISTAS QUE PRESTARÃO OS SERVIÇOS DE OPERAÇÃO IN LOCO

4.1.1. Os analistas de TI que irão operar durante o horário de expediente o ambiente do CFC, conforme Item - ESCOPO DETALHADO DO AMBIENTE PARA PRESTAÇÃO DOS SERVIÇOS DE SUPORTE TÉCNICO, MONITORAMENTO E OPERAÇÃO deverão possuir as qualificações citadas abaixo:

- 4.1.1.1. Analista 01 – Deve possuir Certificação Comptia Network+ válida durante todo o contrato;
- 4.1.1.2. Analista 02 - Deve possuir Certificação Comptia Security+ válida durante todo o contrato;
- 4.1.2. A comprovação de todas as certificações exigidas se dará por meio de apresentação de cópias autenticadas dos certificados emitidos por cada um dos fabricantes ou institutos autorizados pelos mesmos e da carteira de trabalho ou contrato de trabalho do profissional com a empresa contratada no momento da assinatura do contrato.
- 4.1.3. As certificações deverão ainda ser reapresentadas ao Conselho Federal de Contabilidade a cada 06 (seis) meses para comprovar que a Contratada mantém em seu quadro de profissionais os recursos capacitados conforme exigido pelo Contratante.
- 4.1.4. A comprovação de vinculação ao quadro do licitante, na data de assinatura do contrato, se dará por meio de cópias autenticadas das carteiras de trabalho e guias de FGTS quitadas no caso de funcionários, ou ainda do contrato social registrado no órgão competente no caso de sócios. Estes profissionais serão responsáveis pela prestação dos serviços ao ambiente, mencionados no escopo desta proposta.
- 4.1.5. A autenticação dos documentos mencionadas nos subitens 4.1.2 e 4.1.4 poderá ser realizada pelo agente do CFC, em observância a legislações vigentes.

5. COMPETÊNCIAS TÉCNICAS EXIGIDAS DOS ANALISTAS QUE PRESTARÃO OS SERVIÇOS DE OPERAÇÃO REMOTA VIA NOC

- 5.1. O Serviço de operação remota deverá complementar a operação das soluções especificadas conforme Item - ESCOPO DETALHADO DO AMBIENTE PARA PRESTAÇÃO DOS SERVIÇOS DE SUPORTE TÉCNICO, MONITORAMENTO E OPERAÇÃO quando houver necessidade de operação do ambiente fora do expediente quando não houver Analistas presenciais da CONTRATADA no ambiente do CFC.
- 5.2. Os serviços de operação remota deverão ser executados por técnicos da empresa contratada, capacitados com os certificados listados a seguir, de acordo com o serviço ou produto que necessitar de suporte.
- 5.3. No momento da assinatura do contrato, a contratada deverá ter, em seu quadro, pelo menos 2 (dois) funcionários que possuam cada um dos certificados abaixo, bem como a experiência profissional exigida:

- a) MCSE – Microsoft Certified System Engineer – em Windows 2012 ou posterior, para prover suporte ao ambiente Microsoft Windows Server e Active Directory do Conselho Federal de Contabilidade.
- b) Linux LPI, para prover suporte ao ambiente Linux do Conselho Federal de Contabilidade;
- c) ITIL Manager, para prover suporte e metodologia à gestão dos incidentes e problemas do Conselho Federal de

Contabilidade;

d) Forcepoint NGFW Administrator para prover suporte e segurança a solução de firewalls do Conselho Federal de Contabilidade;

e) HCIA-Storage Huawei para prover suporte a solução de armazenamento (storage) em uso;

f) NCDA (NetApp Certified Data Management Administrator), para prover suporte a solução de armazenamento (storage) em uso;

g) Certificação kaspersky Endpoint, para prover suporte na solução de antispam e endpoint do Conselho Federal de Contabilidade;

5.4. A comprovação de todas as certificações exigidas se dará por meio de apresentação de cópias autenticadas dos certificados emitidos por cada um dos fabricantes ou institutos autorizados pelos mesmos e da carteira de trabalho ou contrato de trabalho do profissional com a empresa contratada no momento da assinatura do contrato.

5.5. As certificações deverão ainda ser reapresentadas ao Conselho Federal de Contabilidade a cada 06 (seis) meses para comprovar que a Contratada mantém em seu quadro de profissionais os recursos capacitados conforme exigido pelo Contratante.

5.6. A comprovação de vinculação ao quadro do licitante, na data de assinatura do contrato, se dará por meio de cópias autenticadas das carteiras de trabalho e guias de FGTS quitadas no caso de funcionários, ou ainda do contrato social registrado no órgão competente no caso de sócios. Estes profissionais serão responsáveis pela prestação dos serviços ao ambiente, mencionados no escopo desta proposta.

5.7. autenticação dos documentos mencionadas nos subitens 5.4 e 5.6 poderá ser realizada pelo agente do CFC, em observância a legislações vigentes.

6. SERVIÇO DE SUPORTE TÉCNICO COM MONITORAMENTO 24x7 E OPERAÇÃO DO AMBIENTE DO CFC - ON PREMISE OU EM NUVEM

6.1. CARACTERÍSTICAS GERAIS DO SERVIÇO DE SUPORTE TÉCNICO E MONITORAMENTO 24X7 REMOTO:

6.1.1. Os serviços propostos pela licitante deverão contemplar todos os requisitos descritos nas subseções a seguir.

6.1.2. O regime de atendimento a ser contratado objetiva garantir a disponibilidade, desempenho e segurança do ambiente tecnológico do Conselho Federal de Contabilidade. Sendo assim, a CONTRATADA deverá disponibilizar:

6.1.2.1. Em regime 24x7 (todos os dias do ano) – equipe remota, através do Centro de Operações de Rede (NOC), suficiente para atender aos requisitos de serviços aqui dispostos;

6.1.2.2. A CONTRATADA será responsável por monitorar e suportar toda a infraestrutura de rede, ativos e soluções de segurança, servidores e serviços do Conselho Federal de Contabilidade através de um Centro de Operação de Redes (NOC – Network Operations Center) operando em regime 24x7 durante todos os dias do ano por toda a duração do contrato.

6.1.2.3. O Centro de Operação de Redes (NOC – Network Operations Center) da CONTRATADA deverá atender aos requisitos mínimos de serviços especificados neste termo de referência, bem como TODOS os requisitos de infraestrutura apresentados a seguir:

6.1.2.4. Energia e no-breaks redundantes;

6.1.2.5. Toda a infraestrutura de Tecnologia da Informação do Centro de Operações deverá ser suportada por Grupo Gerador Dedicado com autonomia mínima de 8 (oito) horas sem reabastecimento, no caso de interrupção do fornecimento de energia elétrica;

6.1.2.6. Canais redundantes de comunicação IP dedicados com a Internet, com provedores distintos, com SLA de atendimento igual ou inferior a 04 (quatro) horas para o caso de queda do link e largura de banda mínima de 10 (dez) Mbps. Não serão aceitos contratos com links xDSL, devido ao baixo SLA ofertado pelas operadoras de telecomunicação para este tipo de tecnologia;

6.1.2.7. Sistemas de refrigeração redundantes;

6.1.2.8. Sistema de monitoramento por câmeras;

6.1.2.9. Sistemas de monitoramento e alarme contra incêndio;

6.1.2.10. Firewalls redundantes;

6.1.2.11. Switches redundantes;

6.1.2.12. Roteadores redundantes; e

6.1.2.13. Servidores redundantes ou solução de servidores em lâmina (Blade) para prover os serviços contratados.

6.1.2.14. Utiliza sistema de gerenciamento de CFTV, que viabilizem o rastreamento de pessoas dentro do ambiente da CONTRATADA e cujas imagens possam ser recuperadas;

6.1.2.15. Filmar toda a área, mantendo as imagens armazenadas por 30 (trinta) dias;

6.1.2.16. Efetuar registro de entrada e saída dos visitantes, com identificação individual, em todos os acessos ao NOC;

6.1.2.17. Possuir solução de monitoramento de disponibilidade e desempenho em seu Centro de Operações de Rede e Segurança;

6.1.2.18. O perímetro do NOC deve ser equipado com sensor de intrusão e alarmes contra acesso indevido;

6.1.2.19. O controle de acesso físico ao ambiente do NOC deve ser construído com pelo menos 02 (dois) fatores de autenticação;

6.1.2.20. Disponibilizar sistema via WEB para atendimento, controle e acompanhamento das solicitações de serviços e registros de incidentes

6.1.2.21. Os serviços serão prestados por equipe técnica qualificada e com conhecimento nas soluções existentes no ambiente do CFC listados na tabela do ambiente do CFC a ser gerenciado.

6.1.3. O Conselho Federal de Contabilidade promoverá diligência para checar a veracidade das informações para confrontação do detalhamento das especificações técnicas do termo de referência.

6.2. CARACTERÍSTICAS GERAIS DO SERVIÇO DE OPERAÇÃO REMOTA:

6.2.1. O Conselho Federal de Contabilidade promoverá diligência para checar a veracidade das informações para confrontação do detalhamento das especificações técnicas do termo de referência.

6.2.2. O serviço de administração e operação remota em regime de 16 x 5 em dias úteis (fora do horário de expediente) e 24 x 2 em dias não úteis, prestado pela CONTRATADA deverá realizar, no mínimo, as seguintes atividades:

6.2.2.1. Manter EQUIPE TÉCNICA e RECURSOS DE HARDWARE E SOFTWARE, por meio do seu Centro de Operações de Redes (NOC - Network Operations Center), suficiente para atender o escopo definido e realizar as atividades exigidas, durante o regime de horas estabelecido, TREZENTOS E SESENTA E CINCO DIAS por ano;

6.2.2.2. Receber, diariamente ao final do horário comercial, informações do técnico residente quanto às ocorrências do dia e atividades pendentes que deverão ser assumidas pela equipe remota para atuação;

6.2.2.3. Informar, diariamente, ao início do horário comercial, à equipe residente as ocorrências ocorridas fora do horário comercial, bem como as atividades pendentes que deverão ser assumidas pela equipe residente para atuação;

6.2.2.4. As atividades sob responsabilidade da equipe remota que não puderem ser transferidas para o técnico residente deverão ser continuadas, mesmo em horário comercial, pela equipe remota visando atender aos níveis mínimos de serviço contratados.

6.2.3. Realizar todas as atividades e atender a todos os requisitos descritos para os serviços de:

6.2.3.1. Administração e Operação das Soluções de Segurança; Administração e Operação das Soluções de Infraestrutura de Redes;

6.2.3.2. Administração e Operação dos Servidores, Serviços, Armazenamento e Backup.

6.2.3.3. Apoiar sempre que necessário o desenvolvimento das atividades da equipe residente visando o atendimento dos requisitos do Conselho Federal de Contabilidade;

6.2.4. O Conselho Federal de Contabilidade promoverá diligência para checar a veracidade das informações para confrontação do detalhamento das especificações técnicas do Termo de Referência.

7. ESCOPO DETALHADO DO AMBIENTE PARA PRESTAÇÃO DOS SERVIÇOS DE SUPORTE TÉCNICO, MONITORAMENTO E OPERAÇÃO ON PREMISE OU EM NUVEM Estes serviços deverão ser prestados in loco durante o horário de expediente e remoto após o horário de expediente, conforme regime de horas estabelecido anteriormente.

7.1. SOLUÇÕES DE SEGURANÇA - A Contratada será responsável por administrar e operar todas as soluções de segurança da informação do Conselho Federal de Contabilidade realizando, no mínimo, as atividades descritas a seguir.

7.1.1. Firewalls de Perímetro, Internos, das Regionais e de Escritórios Remotos

7.1.1.1. Operar e configurar os ativos e soluções utilizadas pelo Conselho Federal de Contabilidade incluindo, mas não se limitando a:

- a) Incluir, alterar e remover segmentos de rede;
- b) Incluir, alterar e remover entidades de rede (ex.: hosts, subredes, etc.);
- c) Incluir, alterar e remover políticas (regras) de permissão e bloqueio de acesso;
- d) Incluir, alterar e remover configurações de acesso remoto seguro (túneis de VPN);
- e) Incluir, alterar e remover credenciais de acesso administrativo;
- f) Incluir, ativar e remover módulos de software e hardware que façam parte das soluções;
- g) Parâmetros de monitoramento SNMP;

7.1.1.2. Diagnosticar incidentes de desempenho, disponibilidade e segurança que tenham afetado ou possam ter sido realizados através do ativo;

7.1.1.3. Realizar atividades diárias de manutenção visando garantir os níveis de disponibilidade, desempenho e segurança adequados ao Conselho Federal de Contabilidade;

7.1.1.4. Corrigir eventuais vulnerabilidades identificadas no ambiente;

7.1.1.5. Revisar periodicamente as políticas (regras) de forma a garantir o melhor desempenho da solução, a inexistência de regras não autorizadas ou não mais utilizadas, bem como a conformidade da solução à Política de Segurança da Informação (PSI) do Conselho Federal de Contabilidade;

7.1.1.6. Executar os procedimentos de cópia de segurança (backup) das configurações e versões de software/firmware utilizadas pelos equipamentos administrados;

7.1.1.7. Avaliar e otimizar os parâmetros de configuração para garantir o atendimento aos requisitos de disponibilidade, desempenho e segurança do Conselho Federal de Contabilidade;

7.1.1.8. Verificar, em período a ser definido junto ao Conselho Federal de Contabilidade, a disponibilidade de novas correções, atualizações ou versões de software disponibilizadas pelo fabricante;

7.1.1.9. Aplicar atualizações e correções (patches) disponibilizadas pelo fabricante da solução;

7.1.1.10. Manter a documentação do ambiente periodicamente atualizada.

7.1.2. Sistemas de Detecção/Prevenção de Intrusões (IDS/IPS)

7.1.2.1. Operar e configurar os ativos e soluções utilizadas pelo Conselho Federal de Contabilidade incluindo, mas não se limitando a:

- a) Incluir, alterar e remover segmentos de rede;
- b) Incluir, alterar e remover entidades de rede (ex.: hosts, subredes, etc.);
- c) Incluir, alterar e remover políticas (regras) de permissão e bloqueio de acesso;
- d) Incluir, alterar e remover políticas de proteção contra negação de serviço (DoS);
- e) Incluir, alterar e remover credenciais de acesso administrativo;
- f) Incluir, ativar e remover módulos de software e hardware que façam parte das soluções;
- g) Parâmetros de monitoramento SNMP;

7.1.2.2. Diagnosticar incidentes de desempenho, disponibilidade e segurança que tenham afetado ou possam ter sido realizados através do ativo;

7.1.2.3. Realizar atividades diárias de manutenção visando garantir os níveis de disponibilidade, desempenho e segurança adequados ao Conselho Federal de Contabilidade;

7.1.2.4. Corrigir eventuais vulnerabilidades identificadas no ambiente;

7.1.2.5. Revisar periodicamente as políticas (regras) de forma a garantir o melhor desempenho da solução, a inexistência de regras não autorizadas ou não mais utilizadas, bem como a conformidade da solução à Política de Segurança da Informação (PSI) do Conselho Federal de Contabilidade;

7.1.2.6. Executar os procedimentos de cópia de segurança (backup) das configurações e versões de software/firmware utilizadas pelos equipamentos administrados;

7.1.2.7. Avaliar e otimizar os parâmetros de configuração para garantir o atendimento aos requisitos de disponibilidade, desempenho e segurança do Conselho Federal de Contabilidade;

7.1.2.8. Emitir, sob demanda, relatórios disponibilizados pelas soluções disponibilizadas pelo Conselho Federal de Contabilidade;

7.1.2.9. Personalizar, quando necessário e viável dentro da própria solução, os relatórios de acordo com os requisitos exigidos pelo Conselho Federal de Contabilidade;

7.1.2.10. Verificar, em período a ser definido junto ao Conselho Federal de Contabilidade, a disponibilidade de novas correções, atualizações ou versões de software disponibilizadas pelo fabricante;

7.1.2.11. Aplicar atualizações e correções (patches) disponibilizadas pelo fabricante da solução;

7.1.2.12. Manter a documentação do ambiente periodicamente atualizada.

7.1.3. Segurança do Endpoint – antivírus, IDS/IPS, firewall corporativo para estações de trabalho, notebooks e servidores

7.1.3.1. Operar e configurar os ativos e soluções utilizadas pelo Conselho Federal de Contabilidade incluindo, mas não se limitando a:

- a) Incluir, alterar e remover segmentos de rede;
- b) Incluir, alterar e remover entidades de rede (ex.: hosts e subredes);
- c) Incluir, alterar e remover políticas (regras) de permissão e bloqueio de acesso de firewall;
- d) Incluir, ativar e remover políticas (regras) de permissão e bloqueio de dispositivos USB como, por exemplo, modem 3G;
- e) Incluir, alterar e remover políticas de proteção contra negação de serviço (DoS);
- f) Incluir, alterar e remover credenciais de acesso administrativo;
- g) Incluir, ativar e remover módulos de software e hardware que façam parte das soluções;
- h) Criar pacotes de distribuição de software para os diferentes perfis de clientes (ex.: servidores, estações de trabalho e notebooks) existentes no parque computacional;
- i) Parâmetros de monitoramento SNMP;

7.1.3.2. Diagnosticar incidentes de desempenho, disponibilidade e segurança que tenham afetado ou possam ter sido realizados através do ativo;

7.1.3.3. Realizar atividades diárias de manutenção visando garantir os níveis de disponibilidade, desempenho e segurança adequados ao Conselho Federal de Contabilidade;

7.1.3.4. Corrigir eventuais vulnerabilidades identificadas no ambiente;

7.1.3.5. Revisar periodicamente as políticas (regras) de forma a garantir o melhor desempenho da solução, a inexistência de regras não autorizadas ou não mais utilizadas, bem como a conformidade da solução à Política de Segurança da Informação (PSI) do Conselho Federal de Contabilidade;

7.1.3.6. Executar os procedimentos de cópia de segurança (backup) das configurações e versões de software/firmware utilizadas pelos equipamentos administrados;

7.1.3.7. Avaliar e otimizar os parâmetros de configuração para garantir o atendimento aos requisitos de disponibilidade, desempenho e segurança do Conselho Federal de Contabilidade;

- 7.1.3.8. Emitir, sob demanda, relatórios disponibilizados pelas soluções disponibilizadas pelo Conselho Federal de Contabilidade;
- 7.1.3.9. Personalizar, quando necessário e viável dentro da própria solução, os relatórios de acordo com os requisitos exigidos pelo Conselho Federal de Contabilidade;
- 7.1.3.10. Verificar, em período a ser definido junto ao Conselho Federal de Contabilidade, a disponibilidade de novas correções, atualizações ou versões de software disponibilizadas pelo fabricante;
- 7.1.3.11. Aplicar atualizações e correções (patches) disponibilizadas pelo fabricante da solução;
- 7.1.3.12. Manter a documentação do ambiente periodicamente atualizada.

7.1.4. Antispam e controle de conteúdo para correio eletrônico

- 7.1.4.1. Operar e configurar os ativos e soluções utilizadas pelo Conselho Federal de Contabilidade incluindo, mas não se limitando a:
 - a) Incluir, alterar e remover políticas (regras) de bloqueio (blacklist) e permissão (whitelist) de remetentes e destinatários;
 - b) Incluir, alterar e remover políticas (regras) de permissão, monitoramento e bloqueio de acesso a determinados formatos de arquivos (ex.: Executáveis, Áudio, Vídeo, dentre outros);
 - c) Incluir, alterar e remover políticas (regras) de permissão, monitoramento e bloqueio de palavras chave em corpo de mensagens;
 - d) Incluir, alterar e remover políticas (regras) de quarentena de mensagens;
 - e) Inclusão, alteração e remoção de credenciais de acesso administrativo;
 - f) Inserção, ativação e remoção de módulos de software e hardware que façam parte das soluções;
 - g) Parâmetros de monitoramento SNMP;
- 7.1.4.2. Diagnosticar incidentes de desempenho, disponibilidade e segurança que tenham afetado ou possam ter sido realizados através do ativo;
- 7.1.4.3. Realizar atividades diárias de manutenção visando garantir os níveis de disponibilidade, desempenho e segurança adequados ao Conselho Federal de Contabilidade;
- 7.1.4.4. Corrigir eventuais vulnerabilidades identificadas no ambiente;
- 7.1.4.5. Revisar periodicamente as políticas (regras) de forma a garantir o melhor desempenho da solução, a inexistência de regras não autorizadas ou não mais utilizadas, bem como a conformidade da solução à Política de Segurança da Informação (PSI) do Conselho Federal de Contabilidade;
- 7.1.4.6. Executar os procedimentos de cópia de segurança (backup) das configurações e versões de software/firmware utilizadas pelos equipamentos administrados;
- 7.1.4.7. Avaliar e otimizar os parâmetros de configuração para garantir o atendimento aos requisitos de disponibilidade, desempenho e segurança do Conselho Federal de Contabilidade;
- 7.1.4.8. Emitir, sob demanda, relatórios disponibilizados pelas soluções disponibilizadas pelo Conselho Federal de Contabilidade;
- 7.1.4.9. Personalizar, quando necessário e viável dentro da própria solução, os relatórios de acordo com os requisitos exigidos pelo Conselho Federal de Contabilidade;
- 7.1.4.10. Verificar, em período a ser definido junto ao Conselho Federal de Contabilidade, a disponibilidade de novas correções, atualizações ou versões de software disponibilizadas pelo fabricante;
- 7.1.4.11. Aplicar atualizações e correções (patches) disponibilizadas pelo fabricante da solução;
- 7.1.4.12. Manter a documentação do ambiente periodicamente atualizada.

7.1.5. Controle de conteúdo Web / Proxy

- 7.1.5.1. Operar e configurar os ativos e soluções utilizadas pelo Conselho Federal de Contabilidade incluindo, mas não se limitando a:
 - a) Incluir, alterar e remover políticas (regras) de permissão, monitoramento e bloqueio de acesso à endereços Internet (URLs);
 - b) Incluir, alterar e remover políticas (regras) de permissão, monitoramento e bloqueio de acesso à determinados formatos de arquivos (ex.: Executáveis, Áudio, Vídeo, dentre outros);
 - c) Inclusão, alteração e remoção de credenciais de acesso administrativo;
 - d) Inserção, ativação e remoção de módulos de software e hardware que façam parte das soluções;
 - e) Parâmetros de monitoramento SNMP;
- 7.1.5.2. Diagnosticar incidentes de desempenho, disponibilidade e segurança que tenham afetado ou possam ter sido realizados através do ativo;
- 7.1.5.3. Realizar atividades diárias de manutenção visando garantir os níveis de disponibilidade, desempenho e segurança adequados ao Conselho Federal de Contabilidade;
- 7.1.5.4. Corrigir eventuais vulnerabilidades identificadas no ambiente;
- 7.1.5.5. Revisar periodicamente as políticas (regras) de forma a garantir o melhor desempenho da solução, a inexistência de regras não autorizadas ou não mais utilizadas, bem como a conformidade da solução à Política de Segurança da Informação (PSI) do Conselho Federal de Contabilidade;

- 7.1.5.6. Executar os procedimentos de cópia de segurança (backup) das configurações e versões de software/firmware utilizadas pelos equipamentos administrados;
- 7.1.5.7. Avaliar e otimizar os parâmetros de configuração para garantir o atendimento aos requisitos de disponibilidade, desempenho e segurança do Conselho Federal de Contabilidade;
- 7.1.5.8. Emitir, sob demanda, relatórios disponibilizados pelas soluções disponibilizadas pelo Conselho Federal de Contabilidade;
- 7.1.5.9. Personalizar, quando necessário e viável dentro da própria solução, os relatórios de acordo com os requisitos exigidos pelo Conselho Federal de Contabilidade;
- 7.1.5.10. Verificar, em período a ser definido junto ao Conselho Federal de Contabilidade, a disponibilidade de novas correções, atualizações ou versões de software disponibilizadas pelo fabricante;
- 7.1.5.11. Aplicar atualizações e correções (patches) disponibilizadas pelo fabricante da solução;
- 7.1.5.12. Manter a documentação do ambiente periodicamente atualizada.

7.1.6. Atividades adicionais

- 7.1.6.1. Realizar ações proativas de análise de tráfego de rede Internet, LAN e WAN visando identificar anomalias;
- 7.1.6.2. Emitir ao Conselho Federal de Contabilidade sugestões de melhorias para o ambiente;
- 7.1.6.3. Abrir e acompanhar requisições de serviço (ex.: chamados, tickets e incidentes) junto aos fabricantes das soluções utilizadas pelo Conselho Federal de Contabilidade, bem como coletar informações e executar as ações recomendadas pelos fabricantes;
- 7.1.6.4. Criar e manter atualizados os procedimentos operacionais utilizados para administração e operação das soluções;
- 7.1.6.5. Atuar como suporte de 2º nível para a equipe de Service Desk disponibilizada pela CONTRATADA;
- 7.1.6.6. Acionar, sempre que necessário, o suporte avançado (3º nível) disponibilizado pela CONTRATADA através de seu Centro de Operações de Rede (NOC).

7.2. SOLUÇÕES DE INFRAESTRUTURA DE REDE on premise ou em nuvem A CONTRATADA será responsável por administrar e operar todas as soluções de infraestrutura de rede on premise ou em nuvem (LAN), MAN e WAN do Conselho Federal de Contabilidade realizando, no mínimo, as atividades descritas a seguir:

7.2.1. Topologia e Ativos de Rede LAN, MAN e WAN

7.2.1.1. Revisar, adequar e manter a topologia de rede do Conselho Federal de Contabilidade de acordo com as melhores práticas recomendadas pelos fabricantes dos ativos de rede utilizado, bem como aquelas comumente utilizadas pelo mercado;

7.2.1.2. Operar e configurar os ativos e soluções de rede cabeada utilizadas pelo Conselho Federal de Contabilidade incluindo, mas não se limitando a:

- a) Incluir, alterar e remover redes virtuais locais (VLANs);
- b) Atribuir interfaces (portas) dos switches às VLANs adequada, inclusive configurando-as como trunks de VLANs de acordo com a necessidade;
- c) Ativar e desativar agregações de interfaces (link aggregation) de acordo com a necessidade do ambiente;
- d) Manter o protocolo Spanning-Tree (STP) e suas variantes operacionais dentro do ambiente do Conselho Federal de Contabilidade, de acordo com as melhores práticas para o seu uso;
- e) Incluir, alterar e remover políticas (ACLs) utilizadas para o controle de tráfego;
- f) Inclusão, alteração e remoção de credenciais de acesso administrativo;
- g) Inserção, ativação e remoção de módulos de software e hardware que façam parte das soluções;
- h) Parâmetros de monitoramento SNMP;

7.2.1.3. Operar e configurar os ativos e soluções de rede Wireless (Wireless LAN) utilizadas pelo Conselho Federal de Contabilidade incluindo, mas não se limitando a:

- a) Configurar, operar e manter operacionais controladoras (wireless controllers) e pontos de acesso (AP – access points) wireless que compoñham a infraestrutura de rede sem fio;
- b) Posicionar e reposicionar pontos de acesso wireless visando garantir a melhor cobertura, disponibilidade e desempenho da rede sem fio;
- c) Avaliar periodicamente os níveis de sinal para determinar ações necessárias para garantir os níveis de serviço almejados pelo Conselho Federal de Contabilidade;

7.2.1.4. Diagnosticar incidentes de desempenho, disponibilidade e segurança que tenham afetado ou possam ter sido realizados através do ativo;

7.2.1.5. Realizar atividades diárias de manutenção visando garantir os níveis de disponibilidade, desempenho e segurança adequados ao Conselho Federal de Contabilidade;

7.2.1.6. Corrigir eventuais vulnerabilidades identificadas no ambiente;

7.2.1.7. Revisar periodicamente as políticas (regras) de forma a garantir o melhor desempenho da solução, a inexistência de regras não autorizadas ou não mais utilizadas, bem como a conformidade da solução à Política de Segurança da Informação (PSI) do Conselho Federal de Contabilidade;

7.2.1.8. Executar os procedimentos de cópia de segurança (backup) das configurações e versões de software/firmware utilizadas pelos

equipamentos administrados;

7.2.1.9. Avaliar e otimizar os parâmetros de configuração para garantir o atendimento aos requisitos de disponibilidade, desempenho e segurança do Conselho Federal de Contabilidade;

7.2.1.10. Verificar, em período a ser definido junto ao Conselho Federal de Contabilidade, a disponibilidade de novas correções, atualizações ou versões de software disponibilizadas pelo fabricante;

7.2.1.11. Aplicar atualizações e correções (patches) disponibilizadas pelo fabricante da solução.

7.2.1.12. Avaliar periodicamente e em conjunto com a equipe do Conselho Federal de Contabilidade a topologia utilizada no ambiente de rede, propondo melhorias e o uso de novas tecnologias que possam trazer ganhos para a instituição;

7.2.1.13. Manter a documentação do ambiente periodicamente atualizada.

7.2.2. Serviços de Rede Windows

7.2.2.1. Resolução de Nomes (DNS)

7.2.2.2. Incluir, alterar e remover registros de DNS nos servidores utilizados no ambiente tecnológico do Conselho Federal de Contabilidade;

7.2.2.3. Configurar e manter operacionais os serviços responsáveis pela resolução de nomes, através do protocolo DNS, no ambiente, incluindo:

- a) Criar, alterar e remover registros nos arquivos de zona (ex.: A, CNAME, PTR);
- b) Configurar e manter operacional a replicação de zonas DNS;
- c) Periodicamente realizar a limpeza de registros de DNS não mais utilizados;

7.2.2.4. Diagnosticar incidentes de desempenho, disponibilidade e segurança que tenham afetado ou possam ter sido realizados através do serviço;

7.2.2.5. Manter a documentação do serviço DNS atualizada.

7.2.2.6. Atribuição de Endereçamento IP (DHCP)

7.2.2.7. Incluir, alterar e remover escopos de DHCP nos servidores utilizados no ambiente tecnológico do Conselho Federal de Contabilidade;

7.2.2.8. Configurar e manter operacionais os serviços responsáveis pela atribuição dinâmica de endereços IP, através do protocolo DHCP, no ambiente, incluindo:

7.2.2.9. Criar, alterar e remover escopos de atribuição de endereços;

7.2.2.10. Configurar parâmetros de registros a serem enviados por cada escopo, incluindo a validade das reservas;

7.2.2.11. Configurar reservas e exclusões do escopo de forma a evitar conflitos de endereçamento IP;

7.2.2.12. Periodicamente realizar a limpeza de registros e configurações DHCP não mais utilizadas;

7.2.2.13. Diagnosticar incidentes de desempenho, disponibilidade e segurança que tenham afetado ou possam ter sido realizados através do serviço;

7.2.2.14. Manter a documentação do serviço DHCP atualizada.

7.2.3. Roteamento

7.2.3.1. Incluir, alterar e remover interfaces de roteamento nos ativos aplicáveis;

7.2.3.2. Configurar e manter operacionais as rotas estáticas necessárias para funcionamento do ambiente;

7.2.3.3. Configurar e manter operacionais o protocolo de roteamento dinâmico Open Shortest Path First (OSPF), se necessário para funcionamento do ambiente, incluindo:

- a) Definição de áreas e tipos a serem utilizados;
- b) Parâmetros de autenticação;
- c) Redes participantes;
- d) Configurar e manter, se necessário, políticas (regras) de roteamento para utilização de roteamento baseado em políticas (PBR – Policy Based Routing);

7.2.3.4. Diagnosticar problemas de roteamento nas redes internas e na Internet;

7.2.3.5. Manter a documentação do ambiente periodicamente atualizada.

7.2.4. Atividades adicionais

7.2.4.1. Emitir ao Conselho Federal de Contabilidade sugestões de melhorias para o ambiente;

7.2.4.2. Abrir e acompanhar requisições de serviço (ex.: chamados, tickets e incidentes) junto aos fabricantes das soluções utilizadas pelo Conselho Federal de Contabilidade, bem como coletar informações e executar as ações recomendadas pelos fabricantes;

7.2.4.3. Criar e manter atualizados os procedimentos operacionais utilizados para administração e operação das soluções;

7.2.4.4. Atuar como suporte de 3º nível para a equipe de Service Desk disponibilizada pela LICITANTE;

7.2.4.5. Acionar, sempre que necessário, o suporte avançado (3º nível) disponibilizado pela CONTRATADA através de seu Centro de Operações de Rede (NOC).

7.3. SERVIDORES, SERVIÇOS, ARMAZENAMENTO E BACKUP CONTRATADA será responsável por administrar e operar toda a infraestrutura de rede relacionada a servidores, serviços por eles providos, armazenamento de dados e salvaguarda de dados (backup) realizando, no mínimo, as atividades descritas a seguir.

7.3.1. Servidores

7.3.1.1. Fixar novos servidores que venham a ser adquiridos pelo Conselho Federal de Contabilidade em espaço físico a ser definido nos racks;

7.3.1.2. Verificar periodicamente se todos os cabos de energia, rede lógica e, se aplicável, outros cabos (ex.: HBA, SCSI, etc.) se encontram devidamente fixados;

7.3.1.3. Atualizar periodicamente o inventário de hardware e software dos servidores do Conselho Federal de Contabilidade;

7.3.1.4. Informar à CONTRATANTE sobre eventuais falhas de hardware ou software identificadas e realizar a abertura e acompanhamento de requisições de serviço junto aos fornecedores do produto;

7.3.1.5. Acompanhar o trabalho realizado nas dependências do Conselho Federal de Contabilidade por técnicos dos fornecedores de hardware / software que tenham sido acionados para tratar de eventuais falhas identificadas;

7.3.1.6. Instalar, administrar e manter operacionais os sistemas operacionais que venham a ser instalados nestes servidores incluindo, sistemas Windows Server 2012 ou superiores, e Linux.

7.3.1.7. Recuperar os servidores em caso de falhas incluindo, por exemplo, a reinstalação de sistemas operacionais, reconfiguração de serviços e a recuperação de dados armazenados na solução de salvaguarda de dados do Conselho Federal de Contabilidade;

7.3.1.8. Identificar, controlar e notificar à Contratante tendências de crescimento da utilização dos servidores, visando a gestão proativa do ambiente;

7.3.1.9. A Contratada também deve emitir sugestões de aquisições / atualizações tecnológicas dos recursos.

7.3.2. Serviços. Administrar, operar e configurar os serviços utilizados no ambiente, tais como:

7.3.2.1. Microsoft Active Directory

- a) Administrar e operar o serviço de diretório Active Directory em sua plenitude;
- b) Monitorar e manter operacional a replicação entre os controladores de domínio;
- c) Incluir, alterar e remover diretrizes de grupo (GPO – Group Policy Objects);
- d) Incluir, alterar e remover permissões de arquivos e compartilhamentos de arquivos nos servidores;
- e) Incluir, alterar e remover usuários e grupos no domínio Microsoft Active Directory;
- f) Manter as políticas de tamanho, complexidade e validade de senhas, fundos de tela, dentre outras;
- g) Diagnosticar e resolver problemas de replicação, permissões e outros aplicáveis a um domínio Microsoft Active Directory;
- h) Avaliar periodicamente o funcionamento dos serviços e emitir recomendações de melhoria à Contratante;

7.3.2.2. Microsoft Exchange 2010 ou superior

- a) Administrar e operar o serviço de colaboração Microsoft Exchange em sua plenitude;
- b) Incluir, alterar e remover caixas postais de usuários, grupos e listas de distribuição;
- c) Manter os bancos de dados de caixas postais devidamente dimensionados;
- d) Manter as políticas de limite de tamanho de mensagens e caixas postais;
- e) Diagnosticar e resolver problemas de replicação, permissões, envio e recebimento de mensagens, e outros aplicáveis à solução Microsoft Exchange;
- f) Avaliar periodicamente o funcionamento dos serviços e emitir recomendações de melhoria à CONTRATANTE;

7.3.2.3. Microsoft SQL Server 2012 ou superior

- a) Administrar e operar o serviço de banco de dados Microsoft SQL em sua plenitude;
- b) Incluir, recuperar e remover bancos de dados;
- c) Redimensionar bancos de dados de acordo com os resultados do monitoramento proativo do ambiente;
- d) Incluir, alterar e remover credenciais para acesso à bancos de dados;
- e) NÃO fazem parte do escopo de serviços da CONTRATADA atividades relacionadas ao desenvolvimento de software como, por exemplo:
 - I) Incluir, alterar ou remover tabelas de um banco de dados;
 - II) Incluir, alterar ou remover campos de tabelas;
 - III) Avaliar o conteúdo de tabelas e seus relacionamentos;
 - IV) Diagnosticar problemas de desempenho e otimização de queries SQL;

7.3.2.4. Microsoft Hyper-V e VMware ESX, ESXi e vSphere

- a) Administrar e operar os serviços de virtualização Microsoft e VMware em sua plenitude;
- b) Incluir, alterar, mover e excluir máquinas virtuais (VMs – Virtual Machines);

- c) Configurar as características lógicas de máquinas virtuais como, por exemplo:
- d) Quantidade e capacidade de processadores;
- e) Quantidade de memória RAM virtual;
- f) Quantidade de interfaces de redes e segmentos de rede (ex.: VLAN) aos quais se encontram interligadas;
- g) Quantidade e capacidade dos discos virtuais;
- h) Configurações de inicialização automática ou manual;
- i) Avaliar o ambiente de virtualização periodicamente determinando a melhor distribuição das máquinas virtuais dentro dos servidores físicos visando o melhor aproveitamento dos recursos disponíveis;
- j) Recuperar máquinas virtuais e backups necessários para garantir os níveis de serviço almejados pelo Conselho Federal de Contabilidade;

7.3.2.5. Microsoft Internet Information Services (IIS), Apache HTTPD e Tomcat

7.3.2.6. Administrar e operar os serviços de publicação Web Microsoft e Apache em sua plenitude;

- g) Incluir, alterar e remover publicações de sítios (sites) internos e externos;
- h) Configurar, quando aplicável, o uso de certificados digitais (SSL) para proteção do acesso aos sistemas através do protocolo HTTPS;
- i) Diagnosticar problemas de acesso e permissões na publicação de sítios Web;
- j) Revisar e manter os parâmetros de desempenho das soluções utilizadas;

7.3.2.7. Microsoft Certificate Services (CA)

- a) Administrar e operar os serviços de certificados digitais (autoridade certificadora interna do Conselho Federal de Contabilidade) disponibilizados pelos sistemas operacionais Microsoft Windows;
- b) Emitir, renovar e revogar certificados digitais para computadores, usuários e sítios Web;
- c) Ativar, caso necessário e disponível no ambiente, a distribuição automatizada de certificados digitais de acordo com os requisitos do Conselho Federal de Contabilidade;
- d) Realizar as rotinas de manutenção e salvaguarda de dados da autoridade certificadora;

7.3.2.8. Microsoft Internet Authentication Service (IAS)

- a) Administrar e operar os serviços de autenticação, autorização e contabilidade (AAA – Authentication, Authorization and Accounting) disponibilizados pelo IAS através do protocolo RADIUS;
- b) Incluir, alterar e remover clientes RADIUS e chaves de segurança;
- c) Incluir, alterar e remover políticas de autenticação e autorização de acesso;
- d) Manter operacionais os serviços de autenticação de acordo com os níveis de serviços almejados pelo Conselho Federal de Contabilidade;
- e) Diagnosticar problemas de disponibilidade, desempenho e permissões na solução;

7.3.2.9. Outros

- a) Cadastrar e manter operacionais os compartilhamentos de impressoras de rede, bem como a sua publicação no domínio;
- b) Manter os serviços
- c) A administração, configuração e operação do serviço ERP do Conselho Federal de Contabilidade não faz parte do escopo da CONTRATADA;
- d) A Contratada será responsável, neste caso, apenas pela manutenção do sistema operacional e hardware dos servidores envolvidos no ERP, devendo, em caso de falha, auxiliar a empresa responsável pelo ERP na recuperação dos dados salvaguardados.

7.3.3. Soluções de Armazenamento (Storage)

7.3.3.1. Administrar, configurar e operar as soluções de armazenamento (storage) utilizadas pelo Conselho Federal de Contabilidade;

7.3.3.2. Em caso de falhas de discos a CONTRATADA será responsável por:

- a) Identificar eventuais serviços que tenham sido afetados, notificando a equipe da CONTRATADA;
- b) Abrir e acompanhar solicitações de troca dos discos cobertos por garantia;
- c) Remover os discos defeituosos de acordo com as orientações do fabricante;
- d) Inserir os novos discos de acordo com as orientações do fabricante;
- e) Certificar que os grupos de armazenamento tenham detectado a presença do novo disco e que este tenha sido integrado ao processo de armazenamento, verificando ainda o estado do RAID;

7.3.3.3. Incluir e remover novos volumes e LUNs para acesso dos servidores físicos e virtuais;

7.3.3.4. Redimensionar, quando aplicável e possível, volumes de acordo com os requisitos do Conselho Federal de Contabilidade;

7.3.3.5. Diagnosticar problemas de disponibilidade e desempenho da solução;

7.3.3.6. Movimentar, sob demanda, massas de dados entre um storage e outro;

7.3.3.7. Monitorar o funcionamento da solução visando identificar possíveis falhas e oportunidades de melhoria, bem como tendências de utilização;

7.3.3.8. A Contratante deverá ser notificada com a maior antecedência possível sobre a utilização em excesso deste recurso para que possa avaliar se existem dados a serem removidos ou se realiza um processo de aquisição para expandir o recurso;

7.3.4. Soluções de Salvaguarda de Dados (Backup)

7.3.4.1. Administrar, configurar e operar as soluções de salvaguarda de dados (backup) utilizadas pelo Conselho Federal de Contabilidade;

7.3.4.2. Incluir, alterar e manter configurações de forma a garantir que a Política de Salvaguarda de Dados do Conselho Federal de Contabilidade está sendo atendida;

7.3.4.3. Monitorar o processo de salvaguarda de dados visando identificar eventuais falhas e oportunidades de melhoria de forma a garantir a maior segurança possível ao ambiente do Conselho Federal de Contabilidade;

7.3.4.4. Inserir e remover fitas de backup nas bibliotecas de fitas (tape libraries) e unidades de fita ou em nuvens do Conselho Federal de Contabilidade de forma que os agendamentos de backup (Jobs) possam ser realizados;

7.3.4.5. Certificar que todos os serviços de rede, ativos de infraestrutura e segurança e demais soluções utilizadas pelo Conselho Federal de Contabilidade fazem parte das rotinas de backup da instituição;

7.3.4.6. Realizar testes mensais de recuperação de dados das fitas de backup visando garantir a eficiência e efetividade do processo;

7.3.4.7. Os resultados dos testes deverão ser documentados e apresentados ao gestor do contrato do Conselho Federal de Contabilidade;

7.3.4.8. Realizar, sob demanda, a recuperação de dados de usuários e demais serviços;

7.3.4.9. Atualizar, sempre que necessário e disponível, os agentes de backup utilizados nos servidores.

7.3.4.10. Atuar como suporte de 3º nível para a equipe de Service Desk disponibilizada pela LICITANTE;

7.3.4.11. Acionar, sempre que necessário, o suporte avançado (3º nível) disponibilizado pela CONTRATADA através de seu Centro de Operações de Rede (NOC).

7.4. CARACTERÍSTICAS GERAIS DO SERVIÇO DE MONITORAMENTO DE ATIVOS DE REDE EM REGIME REMOTO 24X7

7.4.1. O serviço deverá monitorar DISPONIBILIDADE, CAPACIDADE E DESEMPENHO, em tempo real e por meio de console centralizado de gerência gráfica via SNMP v1/v2/v3, Netflow, WMI e/ou Requisições a Aplicações, através de ferramenta/soluções que implemente os seguintes requisitos mínimos:

7.4.1.1. Monitoramento de sistemas operacionais Windows Server e Linux;

7.4.1.2. Monitoramento de Banco de Dados SQL;

7.4.1.3. Monitoramento de Correio Eletrônico Microsoft Exchange;

7.4.1.4. Monitoramento de serviços de rede TCP/IP;

7.4.1.5. Monitoramento de Switches, Roteadores e Firewalls;

7.4.1.6. Monitoramento de Storage;

7.4.1.7. Monitoramento de servidores de aplicações web – IIS e Apache;

7.4.1.8. Gerar relatórios estatísticos, por período, de disponibilidade e desempenho;

7.4.1.9. Estabelecer em conjunto com o Conselho Federal de Contabilidade os indicadores de DISPONIBILIDADE, CAPACIDADE e DESEMPENHO a serem monitorados.

7.4.1.10. Ativar, operar e manter atualizada a solução de monitoramento disponibilizada para realizar as atividades previstas, conforme níveis de serviços (SLA) ora estabelecidos.

7.4.1.11. Definir os procedimentos de configuração e ativação de monitoramento via SNMP v1/v2/v3, Netflow, WMI e Requisições a Aplicações para ativos pertencentes ao escopo do contrato.

7.4.1.12. Gerar Relatório de disponibilidade, alertas e desempenho do(s) Serviço(s) Active Directory;

7.4.1.13. Gerar Relatório de disponibilidade, alertas e desempenho do(s) Serviço (s) de Correio Eletrônico;

7.4.1.14. Gerar Relatório de disponibilidade, alertas e desempenho do(s) Serviço(s) de Banco de Dados;

7.4.1.15. Gerar Relatório de disponibilidade, alertas e desempenho de Servidores Windows com serviços monitorados;

7.4.1.16. Gerar Relatório de disponibilidade, alertas e desempenho de Servidores Linux com serviços monitorados;

7.4.1.17. Aspectos da ferramenta de monitoramento e gerência.

7.4.2. Monitorar e analisar em tempo real, em profundidade, as estatísticas de desempenho de rede para routers, switches, pontos de acesso wireless (sem fio), servidores físicos, impressoras, servidores virtuais, nobreaks e quaisquer outros dispositivos habilitados para SNMP nas versões v1, v2 e v3, WMI, e SSH;

7.4.3. A ferramenta deve suportar a realização de inventário dos ativos de rede indicando a conectividade entre os dispositivos, ou seja, deve ser capaz de listar qual dispositivo está conectado em cada uma de suas portas, permitindo traçar mapas de rede; sendo que estes mapas devem ter a capacidade de permitir diagramas customizados pelo usuário. Deve possuir no mínimo as seguintes informações:

- 7.4.3.1. Nome do dispositivo;
- 7.4.3.2. Endereço IP;
- 7.4.3.3. Nome da porta;
- 7.4.3.4. Dispositivo conectado.
- 7.4.4. A ferramenta deve efetuar inventário dos switches da rede indicando:
 - 7.4.4.1. O número total de portas e o status de utilização destas;
 - 7.4.4.2. Status de utilização de Vlan's, indicando quais switches e quais portas fazem parte de determinada Vlan, permitindo listagem por Vlan;
- 7.4.5. Deve ser capaz de indicar quais dispositivos fazem parte de determinada sub-rede;
- 7.4.6. O inventário deve conter no mínimo as seguintes informações através de coletas automáticas:
 - 7.4.6.1. Categoria;
 - 7.4.6.2. Descrição;
 - 7.4.6.3. Tipo de dispositivo;
 - 7.4.6.4. Versão do firmware;
 - 7.4.6.5. Versão do Hardware;
 - 7.4.6.6. Endereço IP;
 - 7.4.6.7. Localização;
 - 7.4.6.8. MAC address;
 - 7.4.6.9. Modelo;
 - 7.4.6.10. SNMP OID;
 - 7.4.6.11. Número de série;
 - 7.4.6.12. Service Tag;
 - 7.4.6.13. Fabricante;
 - 7.4.6.14. Informações de garantia do equipamento;
- 7.4.7. Deve ser capaz de realizar monitoramento de máquinas virtuais, fazendo seu mapeamento e relacionando-as com os equipamentos físicos;
- 7.4.8. A ferramenta deve possibilitar a consulta aos softwares instalados no servidor gerenciado, apresentando no mínimo:
 - 7.4.8.1. Aplicações;
 - 7.4.7.2. Service packs;
 - 7.4.8.3. Patches;
- 7.4.9. Deve ser capaz de gerar gráficos, em tempo real, da utilização de nobreak's, incluindo no mínimo:
 - 7.4.9.1. Tensão de entrada;
 - 7.4.9.2. Tensão de saída;
 - 7.4.9.3. Carga disponível;
 - 7.4.9.4. Corrente de saída;
 - 7.4.9.5. Alertas para queda e variação de energia;
- 7.4.10. Permitir efetuar coletas nos sistemas operacionais (todos nas plataformas 32 e 64 bits):
 - 7.4.10.1. Windows (2000, 2003, 2008, 2012, XP, VISTA, SEVEN, 8 ou superiores);
 - 7.4.10.2. Linux (Debian, Suse, Red Hat);
 - 7.4.10.3. BSD (FreeBSD, OpenBSD);
 - 7.4.10.4. UNIX;
- 7.4.11. Fornecer dados históricos para fins de planejamento de capacidade, com armazenamento por período mínimo de um ano;
- 7.4.12. Fornecer informações sobre interrupções ou inoperâncias por meio de cores e/ou formato de ícones, informando se os elementos estão ou não ativos, e se os parâmetros estão ou não dentro dos limites preestabelecidos;
- 7.4.13. Deve realizar o descobrimento automático de equipamentos e serviços de rede;
- 7.4.14. Realizar descobrimento automático da topologia de nível 2 e nível 3 da rede para apresentação do mapa de conectividade e de informações de configurações dos elementos. O descobrimento de nível 2 deverá suportar pelo menos os seguintes métodos de pesquisa:
 - 7.4.14.1. Consulta a tabelas ARP;
 - 7.4.14.2. Consulta a tabelas de endereçamento IP;
 - 7.4.14.3. Consulta a tabelas de protocolos de código-aberto e proprietários de descobrimento;

- 7.4.14.4. Consultar as tabelas de roteamento;
- 7.4.14.5. Efetuar “polling” dos elementos de rede em intervalos configuráveis;
- 7.4.14.6. Representar graficamente o estado de cada um dos elementos pesquisados;
- 7.4.14.7. Acompanhar o desempenho dos links contratados em tempo real;
- 7.4.14.8. Permitir a criação de grupos de dispositivos, interfaces ou grupos e análise de disponibilidade dos mesmos;
- 7.4.14.9. Permitir a correlação de eventos através da criação de dependências entre grupos e dispositivos de rede;
- 7.4.15. Habilitar alertas avançados para eventos correlacionados, condições mantidas e combinações complexas de estados de dispositivos. Devendo incluir pelo menos:
 - 7.4.15.1. Causa da falha;
 - 7.4.15.2. Severidade;
 - 7.4.15.3. Hora de início e fim;
 - 7.4.15.4. Descrição do dispositivo;
 - 7.4.15.5. Endereço IP;
 - 7.4.15.6. As notificações devem suportar no mínimo os seguintes formatos:
 - a) E-mail;
 - b) Pages;
 - c) SNMP Traps;
 - d) SMS;
 - e) Execução de aplicações externas;
 - f) Anexo
 - g) Mensagens de Syslog;
 - h) Execução de scripts;
 - i) Start e restart de serviços;
- 7.4.16. Permitir a categorização dos ativos de rede por cidade, estado, país ou departamento, assim como a criação de novas categorias para a classificação dos mesmos;
- 7.4.17. Utilizar um monitor universal de dispositivos para monitorar qualquer equipamento habilitado para SNMP;
- 7.4.18. Permitir acréscimo de monitoramentos personalizados através da inclusão de MIB's no sistema;
- 7.4.19. Conter mecanismos ou ferramentas inclusas de MIB Walker, MIB Explorer e Gerenciador de MIB's SNMP;
- 7.4.20. Permitir o desenho e mapeamento da topologia da rede informando as ligações e conexões entre dispositivos;
- 7.4.21. Monitorar servidores virtualizados na plataforma VMWARE e automaticamente acompanhar seu desempenho através de integração com o vCenter;
- 7.4.22. Possuir um centro de mensagens único para todos os alertas de eventos em dispositivos e/ou serviços de maneira a permitir correlação desses eventos;
- 7.4.23. Permitir a configuração ou agendamento de descobrimento automático na rede;
- 7.4.24. Permitir a criação de relatórios de rede personalizados que possam ser exportados para pdf, planilha, impresso ou visualizado via HTTP;
- 7.4.25. Possuir ferramenta de gerenciamento remoto através de dispositivos móveis Android e IOS;
- 7.4.26. Permitir adição de mapas gráficos escolhendo entre vários modelos integrados geograficamente ou importar imagem lógica da rede;
- 7.4.27. Deve suportar IPV4 e IPV6;
- 7.4.28. Deve possibilitar a consulta da tabela de usuários ativos nos equipamentos;
- 7.4.29. Deve permitir mapeamento de usuários logados em determinados períodos assim como traçar um histórico dos logons efetuados ao longo do tempo;
- 7.4.30. Deve permitir a criação de whitelists de equipamentos com inclusão automática através de regras e emissão de alertas quando equipamentos que não fazem parte desta whitelist se conectarem a rede;
- 7.4.31. Deve possibilitar a consulta de tabela das interfaces de rede, incluindo nome, velocidade, status, tráfego de entrada e saída e erros de entrada e saída, assim como descartes de pacotes nas interfaces;
- 7.4.32. Deve possibilitar a consulta de informações da tabela ARP, tanto IPV4 quanto IPV6;
- 7.4.33. Deve possibilitar a consulta da tabela de roteamento, tanto IPV4, quanto IPV6;
- 7.4.34. Deve possibilitar a consulta a informações de desempenho do sistema gerenciado, incluindo:
 - 7.4.34.1. Memória utilizada (valor absoluto e percentual);
 - 7.4.34.2. Swap utilizado (valor absoluto e percentual);

- 7.4.34.3. Taxa de buffer I/O;
- 7.4.34.4. Carga de CPU;
- 7.4.34.5. Utilização de CPU em percentual, incluindo Idle, User, System e Wait;
- 7.4.34.6. Utilização de partições de disco, em valor absoluto e percentual;
- 7.4.34.7. Estatísticas dos discos físicos, incluindo quantidade de leituras e escritas;
- 7.4.34.8. Tabela dos principais processos do sistema;
- 7.4.35. A ferramenta deve ser capaz de executar análise em tempo real possibilitando:
 - 7.4.35.1. Selecionar um grupo de dispositivos e consultar uma variável do dispositivo a intervalos regulares de tempo e colocar os valores em gráficos;
 - 7.4.35.2. Selecionar um grupo de variáveis de um dispositivo e consultar o seu valor a intervalos regulares de tempo e colocar esses valores em gráficos;
 - 7.4.35.3. Incluir os valores em um único gráfico ou em vários gráficos;
 - 7.4.35.4. Obter informação histórica pelo menos 1 hora antes de iniciar a análise em tempo real;
 - 7.4.35.5. Gravar estes perfis de análise em tempo real para o seu uso posterior;
 - 7.4.35.6. Deve também ser compatível com acessos a bancos de dados Microsoft SQL Server, deve incluir ferramenta que execute teste de ping através do protocolo ICMP, gerenciamento de Cluster Microsoft, Internet Information Services (IIS) e Microsoft Active Directory (AD);
- 7.4.36. Os recursos de monitoramento e alertas via dispositivo móvel devem ser executados através do uso de um único módulo. Não serão aceitas soluções que necessitem instalação de ferramentas e aplicativos de terceiros.
- 7.4.37. Prover métricas de monitoração de Aplicações:
 - 7.4.37.1. Monitorar Aplicações sem a necessidade de instalação de agentes;
 - 7.4.37.2. Monitorar / Adicionar, Aplicações através de Discovery;
 - 7.4.37.3. Monitorar transação das aplicações monitoradas;
 - 7.4.37.4. Monitorar Métricas do Microsoft Active Directory;
 - 7.4.37.5. Monitorar Métricas do Microsoft Exchange;
 - 7.4.37.6. Monitorar Métricas de Web Server;
- 7.4.38. Prover Possibilidade de correlação do Servidor de Aplicação com a Aplicação Monitorada, gerando a possibilidade de alertas, com base em um incidente gerado a partir do servidor de aplicação;
- 7.4.39. Prover flexibilidade de edição e adição de métricas, para cada Aplicação e/ou Serviços;
- 7.4.40. Prover Monitoração de Falhas e Performance de Servidores:
 - 7.4.40.1. Monitorar Servidores sem a necessidade de instalação de agentes;
 - 7.4.40.2. Monitorar Falhas e eventos de Servidores;
 - 7.4.40.3. Monitorar Componentes de Hardware de Servidores;
- 7.4.41. Monitorar Métricas de Performance como:
 - 7.4.41.1. Utilização de CPU e vCPU;
 - 7.4.41.2. Utilização de Memória Física e Virtual;
 - 7.4.41.3. Utilização de Volumes (Discos);
 - 7.4.41.4. Utilização de Interfaces de Rede;
 - 7.4.41.5. Monitoração de Perda de Pacotes e Tempo de Resposta;
 - 7.4.41.6. Monitorar Windows Event logs;
 - 7.4.41.7. Monitorar Serviços em Tempo Real;
- 7.4.42. Prover visão Topológica;
- 7.4.43. Prover possibilidade de execução de "Trace Route", a partir de interface gráfica;
- 7.4.44. Prover console de Alerta unificada.



Conselho Regional de Contabilidade do Estado de São Paulo

CONTRATO CRC SP Nº 037/2021

CONTRATO DE PRESTAÇÃO DE SERVIÇOS DE MONITORAMENTO DE SEGURANÇA DA INFORMAÇÃO (CSOC)

CONTRATANTE: CONSELHO REGIONAL DE CONTABILIDADE DO ESTADO DE SÃO PAULO, autarquia federal criada pelo Decreto-Lei nº 9.295/46, inscrito no CNPJ/MF sob o nº 63.002.141/0001-63, com sede na Rua Rosa e Silva, 60, Higienópolis, São Paulo SP, CEP 01230-020, neste ato representado pelo seu Presidente, o Contador José Donizete Valentina.

CONTRATADA: ISH TECNOLOGIA S.A., inscrita no CNPJ/MF sob o nº 01.707.536/0001-04, com sede na Rua Judith Maria Tovar Varejão, 355, Sala 202 e 203, Enseada do Sua, Vitória ES, CEP 29050-360, representada pelo seu procurador, Senhor Renato Tenório, de acordo com a representação legal que lhe é outorgado por procuração.

As partes têm entre si justo e avençado, e celebram o presente contrato, instruído no Processo Compras nº 029/2021, mediante as cláusulas e condições que se seguem:

CLÁUSULA PRIMEIRA – DO OBJETO

1. O presente contrato tem por teor a prestação de serviços de monitoramento de segurança da informação (CSOC).
2. A especificação técnica constitui o objeto mínimo a ser executado pela CONTRATADA, ficando claro que essa execução não exime o prestador dos serviços do emprego de outras posturas técnicas e dos materiais necessários ao pleno alcance das finalidades do presente contrato, ainda que não descritas expressamente.
3. A prestação dos serviços implica, obrigatoriamente, o fornecimento por parte da CONTRATADA de todo o material necessário para o cumprimento do objeto do contrato.

CLÁUSULA SEGUNDA – DO VALOR DO CONTRATO

- 1.1. O valor total estimado deste contrato é de R\$ 1.278.000,00 (um milhão, duzentos e setenta e oito mil reais), dividido em 36 parcelas de R\$ 35.500,00 (trinta e cinco mil e quinhentos reais) mensais;
1. O valor estimado do contrato inclui todas as despesas diretas e indiretas necessárias à fiel execução do objeto pactuado, tais como, tributos, despesas e contribuições com

Página 1 de 10



pessoal, material e outros itens diretamente ligados à viabilização da prestação do serviço.

CLÁUSULA TERCEIRA – DA DESPESA E DOS CRÉDITOS ORÇAMENTÁRIOS

1. A despesa orçamentária da execução deste contrato correrá à Conta de Despesa nº 63130201005 – Serviços de Tecnologia da Informação, mediante a emissão da Nota de Reserva Orçamentária nº 003695.

CLÁUSULA QUARTA – DA VIGÊNCIA

1. O prazo de vigência do presente contrato será de 36 (trinta e seis) meses, contados a partir da data de assinatura, sendo que a execução de cada etapa dos trabalhos se dará segundo cronograma de datas oportunamente desenvolvido pelas partes, não se admitindo, ainda, a dilação dos prazos ali previstos, salvo no caso de apresentação de justificativa que demonstre, de forma circunstanciada, que as causas do atraso são totalmente alheias à vontade do CONTRATADO.

CLÁUSULA QUINTA – DA EXECUÇÃO DOS SERVIÇOS

1. A execução dos serviços deverá manter conformidade com o Anexo VI do Edital de Pregão Eletrônico nº 011/2021.

CLÁUSULA SEXTA – DO PAGAMENTO

1. O pagamento será efetuado mensalmente, após 10 (dez) dias do período de fechamento da prestação dos serviços, mediante a apresentação de relatórios dos serviços efetuados, e dos documentos hábeis para efetivação do pagamento e aceite pelo departamento gestor do contrato.
 - 1.1. Será considerado período de fechamento, o mês comercial de 30 (trinta) dias, com início na data de vigência do contrato e termino no último dia do mês subsequente.
1. Para tanto o documento de cobrança deverá ser entregue pelo CONTRATADO aos cuidados do Departamento de Compras e Licitações do CONTRATANTE, acompanhado, inclusive, do boleto bancário necessário para dar liquidação da despesa, quando for o caso, sempre observando o prazo constante da respectiva proposta e exigências legais.
2. O documento de cobrança será emitido em nome do CONSELHO REGIONAL DE CONTABILIDADE DO ESTADO DE SÃO PAULO, sem rasuras, devendo, conter, ainda, todos os dados do CONTRATADO e outros conforme abaixo especificado:





Conselho Regional de Contabilidade do Estado de São Paulo

- 2.1. O número de inscrição no CNPJ/MF do CONTRATADO deverá ser o mesmo da documentação apresentada para habilitação, da proposta comercial e do documento de cobrança;
- 2.2. Havendo divergência entre o CNPJ/MF, o CONTRATADO deverá juntar declaração justificando tal procedimento, responsabilizando-se, ainda, pela regularidade fiscal do estabelecimento emissor do documento de cobrança;
- 2.3. Os pagamentos efetuados pelo CONTRATANTE estão sujeitos ao disposto no artigo 64, da Lei nº 9.430/96;
- 2.4. A nota fiscal deverá ser emitida, já constando todos os impostos e/ou tributos incidentes, nos termos da IN RFB nº 1.234/12;
- 2.5. Caso o CONTRATADO seja optante pelo "SIMPLES", deverá juntar a declaração original de isenção dos impostos, em 02 (duas) vias, devidamente assinada com identificação do assinante;
- 2.6. A supracitada declaração deverá ser juntada, individualmente, a cada emissão de nota fiscal;
- 2.7. Relatório Mensal das atividades desenvolvidas;
- 2.8. Nenhum pagamento será efetuado ao CONTRATADO sem apresentação das certidões de regularidade fiscal perante a Seguridade Social, o Fundo de Garantia por Tempo de Serviço, a Receita Federal do Brasil e a Justiça do Trabalho.
3. Caso o CONTRATADO deixe de atender, mesmo que de forma parcial, as regras contidas nesta cláusula, o pagamento ficará retido até seu pleno atendimento e não caracterizará, em hipótese alguma, inadimplência por parte do CONTRATANTE.
4. O CONTRATANTE poderá deduzir da nota fiscal/fatura de serviços, do montante a pagar, os valores correspondentes a multas, ressarcimento de despesas ou indenizações devidas pela CONTRATADA, nos termos deste contrato.
5. Ocorrendo eventuais atrasos de pagamento, desde que a CONTRATADA não tenha concorrido de alguma forma para tanto, fica convencionado que os encargos moratórios devidos pelo CONTRATANTE, entre a data prevista para pagamento e a correspondente ao efetivo pagamento da nota fiscal/fatura, a serem incluídos na fatura do mês seguinte ao da ocorrência, são calculados por meio da aplicação da seguinte fórmula aritmética:

$$EM = N \times VP \times I$$
 onde:

EM = Encargos moratórios;

N = Numero de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga;

I = Índice de compensação financeira, assim apurado: $I = (TX/100)/365$



Onde TX = percentual da taxa acumulada dos últimos 12 (doze) meses do fato em que se deu o atraso.

- a) Será utilizado o Índice de Preços ao Consumidor Ampliado (IPCA) do Instituto Brasileiro de Geografia e Estatística (IBGE) e
- b) Na descontinuidade da apuração/divulgação do referido índice, o CONTRATANTE elegerá outro índice da mesma instituição.

CLÁUSULA SÉTIMA – DO ACOMPANHAMENTO

1. Durante a vigência deste contrato, o acompanhamento da prestação de serviços terão como representante do CONTRATANTE o Gerente do Departamento de Tecnologia da Informação, que exigirá o fiel cumprimento das especificações técnicas contratadas, sendo, ainda, permitida a assistência de terceiros, sob pena de não liberação do pagamento previsto neste contrato, inclusive até a conclusão do processo administrativo próprio, se for o caso.
2. O representante do CONTRATANTE pode sustar qualquer trabalho que esteja sendo executado em desacordo com o especificado, sempre que essa medida se tornar necessária.
3. A atestação de conformidade cabe ao titular do departamento responsável e fiscalização do contrato ou a outro funcionário designado para esse fim.

CLÁUSULA OITAVA – DAS OBRIGAÇÕES DO CONTRATANTE

1. Cabe ao CONTRATANTE:
 - 1.1. Permitir acesso dos empregados da CONTRATADA às dependências do CONTRATANTE, quando necessário, para a prestação dos serviços;
 - 1.2. Prestar as informações e os esclarecimentos pertinentes que venham a ser solicitados pelo representante da CONTRATADA;
 - 1.3. Fornecer em tempo hábil, todos os elementos necessários para a prestação dos serviços/fornecimento dos produtos;
 - 1.4. Notificar imediatamente a CONTRATADA sobre qualquer condição operacional anormal;
 - 1.5. Efetuar o pagamento devido, segundo as condições estabelecidas.
 - 1.6. Oferecer informações à CONTRATADA, sempre que necessárias para execução dos trabalhos.

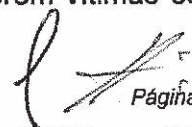


**CLÁUSULA NONA – DAS OBRIGAÇÕES DA CONTRATADA****1. Cabe à CONTRATADA o cumprimento das seguintes obrigações:**

- 1.1. Responder, em relação aos seus funcionários, por todas as despesas decorrentes do fornecimento dos produtos e por outras correlatas, tais como salários, seguros de acidentes, tributos, indenizações, vales refeição, vales transporte e outras que porventura venham a ser criadas e exigidas pelo Poder Público;
- 1.2. Respeitar as normas e procedimentos de controle interno, inclusive de acesso às dependências do CONTRATANTE e do local de entrega dos produtos;
- 1.3. Responder pelos danos causados diretamente à Administração ou aos bens do CONTRATANTE, ou ainda a terceiros, decorrentes de sua culpa ou dolo, durante a execução do contrato, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo CONTRATANTE;
- 1.4. Efetuar a troca dos produtos/serviços que não atenderem às especificações do objeto, no prazo assinado pela Administração do CONTRATANTE;
- 1.5. Comunicar à Administração do CONTRATANTE qualquer anormalidade constatada e prestar os esclarecimentos solicitados;
- 1.6. Manter, durante o período de vigência do Contrato, o atendimento das condições de habilitação exigidas no Edital do Pregão Eletrônico nº 011/2021.
- 1.7. cumprir todos os prazos fixados, de acordo com as exigências dispostas nos Anexos I e VI do Edital do Pregão Eletrônico nº 011/2021, bem como em obediência àqueles que forem acordados com a representante da CONTRATANTE;
- 1.8. manter a documentação apresentada para habilitação em compatibilidade com as obrigações assumidas, em especial aquelas pertinentes à regularidade fiscal perante a Seguridade Social, Fundo de Garantia por Tempo de Serviço, Receita Federal do Brasil e Justiça Trabalhista;
- 1.9. independentemente de transcrição, sujeitar-se às demais obrigações estabelecidas nos Anexos I e VI do Edital do Pregão Eletrônico nº 011/2021.

2. Cabe à CONTRATADA assumir ainda a responsabilidade pelas seguintes obrigações:

- 2.1. todos os encargos previdenciários e obrigações sociais previstos na legislação social e trabalhista em vigor, obrigando-se a saldá-los na época própria, vez que os seus empregados não manterão nenhum vínculo empregatício com o CONTRATANTE;
- 2.2. todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrência da espécie, forem vítimas os seus

 **Página 5 de 10**



empregados durante a execução deste contrato, ainda que acontecido em dependência do CONTRATANTE;

- 2.3. todos os encargos de possível demanda trabalhista, civil ou penal, relacionada à execução deste contrato, originariamente ou vinculada por prevenção, conexão ou continência;
 - 2.4. encargos fiscais e comerciais resultantes desta contratação;
 - 2.5. obrigar-se, quando solicitada, a prestar esclarecimentos e atender prontamente as reclamações que lhe for dirigida.
 - 2.6. dar ciência ao CONTRATANTE, imediatamente, por escrito, de qualquer anormalidade que verificar quanto ao objeto deste instrumento;
 - 2.7. responder por todos e quaisquer danos pessoais ou materiais causados por seus profissionais ou prepostos às dependências, instalações e equipamentos do CONTRATANTE e de terceiros, a título de culpa ou dolo, providenciando a correspondente indenização, assim como arcar com despesas decorrentes de quaisquer infrações praticadas por seu pessoal durante a prestação dos serviços, ainda que no recinto do CONTRATANTE, além de multas ou despesas de qualquer natureza.
 - 2.8. dar imediato conhecimento ao CONTRATANTE sobre qualquer fato extraordinário ou anormal que ocorrer durante toda a execução do objeto contratado.
3. São expressamente vedadas à CONTRATADA:
- 3.1. A contratação de funcionário pertencente ao quadro de pessoal do CONTRATANTE durante a vigência deste contrato;
 - 3.2. a veiculação de publicidade acerca deste contrato, salvo se houver prévia autorização da Administração do CONTRATANTE; e
 - 3.3. a subcontratação de outra empresa para a execução total ou parcial do objeto deste contrato.
4. A inadimplência da CONTRATADA, com referência aos encargos estabelecidos neste contrato, não transfere a responsabilidade por seu pagamento à Administração do CONTRATANTE, nem pode onerar o objeto deste contrato, razão pela qual a CONTRATADA renuncia expressamente a qualquer vínculo de solidariedade, ativa ou passiva, com o CONTRATANTE.

CLÁUSULA DÉCIMA – DAS PENALIDADES

1. A CONTRATADA ficará sujeita, no caso de atraso injustificado, assim considerado pelo CONTRATANTE, inexecução parcial ou inexecução total da obrigação, sem prejuízo das





Conselho Regional de Contabilidade do Estado de São Paulo

responsabilidades civil e criminal, sendo assegurado o contraditório e a ampla defesa, às seguintes penalidades:

- 1.1. advertência;
- 1.2. multa de:
 - a) 3% (três por cento) ao dia sobre o valor atualizado do contrato, limitada a incidência a 05 (cinco) dias. Decorrido o prazo e a critério do CONSELHO, no caso de cumprimento com atraso, poderá ocorrer a não aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença;
 - b) 5% (cinco por cento) ao dia sobre o valor mensal do contrato no caso de atraso na prestação de qualquer obrigação contratual, limitada a incidência a 05 (cinco) dias;
 - c) 20% (vinte por cento) sobre o valor atualizado do contrato, em caso de atraso no cumprimento, por período superior ao previsto no item "a", ou de inexecução parcial da obrigação assumida;
 - d) 30% (trinta por cento) sobre o valor atualizado do contrato, em caso de inexecução total da obrigação assumida, não estando prejudicada a adoção dos procedimentos necessários para a devolução do montante pago à CONTRATADA;
 - e) nos casos previstos nos itens acima a multa será acrescida de juros de 1% (um por cento) ao mês até a data do efetivo pagamento;
- 1.3. suspensão temporária de participar de licitação e impedimento de contratar com o CONTRATANTE.
- 1.4. declaração de inidoneidade da CONTRATADA para licitar ou contratar com a administração pública, em função da natureza ou gravidade da falta cometida, sem prejuízo da aplicação das multas.
2. A sanção de multa poderá ser aplicada à CONTRATADA juntamente com a advertência, declaração de inidoneidade, suspensão temporária para licitar e contratar com o CONTRATANTE, descontando-a do pagamento a ser efetuado, se for o caso.

CLÁUSULA DÉCIMA PRIMEIRA – DA PRORROGAÇÃO

1. Caso se verifique justificada a necessidade e o CONTRATANTE entenda conveniente e vantajosa a prorrogação do presente instrumento contratual, o CONTRATANTE deverá manifestar tal intenção expressamente à CONTRATADA, respeitando-se os preceitos e limites descritos no artigo 57 da Lei nº 8.666/93.



CLÁUSULA DÉCIMA SEGUNDA – DO REAJUSTE DO CONTRATO

1. A repactuação e o reajuste serão permitidos, desde que observado o interregno mínimo de 12 (doze) meses, contados a partir da assinatura deste contrato ou da data do último reajuste/repactuação.
2. O reajuste será efetuado de acordo com o índice IPCA-IBGE.

CLÁUSULA DÉCIMA TERCEIRA – DAS ALTERAÇÕES

1. Havendo justificada necessidade, o presente contrato poderá ser alterado, respeitados os preceitos do artigo 65 da Lei nº 8.666/93.

CLÁUSULA DÉCIMA QUARTA – DA RESCISÃO

1. A inexecução total ou parcial deste instrumento contratual enseja a sua rescisão, podendo ser:
 - 1.1. por iniciativa do CONTRATANTE, independentemente de interpelação judicial ou extrajudicial, a infração por parte da CONTRATADA de qualquer cláusula ou condição do contrato ou a ocorrência de quaisquer situações previstas nos artigos 78 e 79 da Lei nº 8.666/93.
 - 1.2. por iniciativa da CONTRATADA, a inobservância por parte do CONTRATANTE quanto ao pagamento estabelecido neste instrumento, salvo por fundamentação e comprovação administrativas escusáveis, nos termos dos artigos 78 e 79 da Lei nº 8.666/93.
 - 1.3. amigável, após acordo entre as partes, reduzida a termo no processo administrativo, desde que haja conveniência para o CONTRATANTE;
2. A rescisão administrativa ou amigável deverá ser precedida de autorização escrita e fundamentada da autoridade competente.
3. Os casos de rescisão contratual serão formalmente motivados nos autos do processo, assegurado o contraditório e a ampla defesa.
4. No caso de rescisão provocada por inadimplemento do CONTRATADO, o CONTRATANTE poderá reter, cautelarmente, os créditos decorrentes do contrato até o valor dos prejuízos causados, já calculados ou estimados.

CLÁUSULA DÉCIMA QUINTA – DA TOLERÂNCIA

1. Qualquer tolerância das partes no cumprimento, no todo ou em parte, de qualquer das cláusulas e/ou condições contratuais, será considerada como concessão excepcional,





Conselho Regional de Contabilidade do Estado de São Paulo

não constituindo inovação do aqui ajustado, nem precedente invocável pela CONTRATADA.

CLÁUSULA DÉCIMA SEXTA – DA FUNDAMENTAÇÃO LEGAL E DA VINCULAÇÃO À PROPOSTA

1. O presente contrato fundamenta-se na Lei nº 8.666/93;
2. O presente contrato vincula-se aos termos:
 - 2.1. do Edital do Pregão Eletrônico nº 011/2021, bem como do(s) seu(s) anexo(s), que fazem parte do Processo Compras nº 029/2021; e
 - 2.2. da proposta vencedora da CONTRATADA.

CLÁUSULA DÉCIMA SÉTIMA – DA CONFIDENCIALIDADE

1. Os empregados e/ou prepostos da CONTRATADA, ater-se-ão com zelo aos limites de suas tarefas.
2. Ocorrendo violação, divulgação, vazamento de dados ou qualquer infração ao disposto na Lei nº 13.709/2018 a CONTRATADA, responderá por perdas e danos na forma da lei, além de eventuais aspectos criminais envolvidos.

CLÁUSULA DÉCIMA OITAVA – DA RESPONSABILIDADE CIVIL

1. A CONTRATADA reconhece por este instrumento que é a única e exclusiva responsável por danos ou prejuízos que vier a causar ao CONTRATANTE, coisa, propriedade ou pessoa de terceiros, em decorrência de execução dos serviços, ou danos advindos de qualquer comportamento de seus empregados em serviço, objeto deste contrato, correndo às suas expensas, sem quaisquer ônus para o CONTRATANTE, ressarcimento ou indenizações que tais danos ou prejuízos possam causar.

CLÁUSULA DÉCIMA NONA – DO FORO

1. As questões decorrentes da execução deste Instrumento, que não possam ser dirimidas administrativamente, serão processadas e julgadas na Justiça Federal, no Foro da cidade de São Paulo SP, Seção Judiciária de São Paulo, com renúncia de qualquer outro por mais privilegiado que seja.



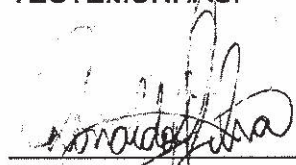
E, para firmeza e validade do que foi pactuado, lavrou-se o presente Contrato em 02 (duas) vias de igual teor e forma, para que surtam um só efeito, as quais, depois de lidas, são assinadas pelos representantes das partes, CONTRATANTE e CONTRATADA, e pelas testemunhas abaixo, devidamente qualificadas.

São Paulo, 04 de outubro de 2021.


CONTRATANTE
José Donizete Valentina
Presidente


CONTRATADA
Renato Tenório
Procurador
Renato Tenório
Diretor Executivo
RG.: 19.953.787-2
ISH TECNOLOGIA S.A.

TESTEMUNHAS:


RONALDO CESAR DA SILVA
Gerente de TI - CRC SP


Jefferson Di Lorenzo Gasco
Analista Administrativo



ANEXO VI
PREGÃO ELETRÔNICO 011/2021

DESCRIPTIVO TÉCNICO

A solução contempla a contratação de empresa para a Prestação de serviços de monitoramento de segurança (CSOC);

ESPECIFICAÇÕES DO OBJETO

1. DETALHAMENTO DO OBJETO:

Serviços Gerenciados de Segurança, envolvendo prestação de serviços de:

- 1.1 Serviços de monitoramento de ataques cibernéticos, visa o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados ao CONTRATANTE, através de correlacionamento de logs, pacotes de redes, e/ou comportamento anômalo de aplicações, serviços e infraestrutura do CONTRATANTE, que possam gerar eventos de segurança da informação, aos quais devem ser analisados, podendo estes serem transformados em um incidente de segurança da informação, obedecendo um processo cíclico e rigoroso de gestão de eventos.
- 1.2 Serviços de resposta a incidentes de segurança, para analisar, remediar, conter e documentar os eventos de segurança da informação, que após analisados se descobriu que de fato era um ataque iminente ao CONTRATANTE, e foram transformados em um incidente de segurança da informação. Tal serviço deverá ser executado através de um **CSOC** do inglês **Cyber Security Operations Center**, obedecendo os principais frameworks de resposta a incidente de segurança da informação, e boas práticas de mercado já conhecidas.
- 1.3 Todos os serviços descritos pertencem a um único objeto e bloco de contratação denominado SERVIÇOS GERENCIADOS DE SEGURANÇA. Todas as características e requisitos exigidos nesse termo de referência serão confirmadas em diligência presencial.

2. QUANTO AO OBJETO DA CONTRATAÇÃO

- 2.1 São apresentadas, a seguir, especificações técnicas mínimas dos serviços a serem ofertados referentes ao objeto. Os termos “possui”, “permite”, “suporta” e “é” implicam no fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo “ou” implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo “e” implica que a

especificação técnica mínima dos serviços deve ser atendida englobando todas as opções.

2.2 O objeto de contratação dos SERVIÇOS GERENCIADOS DE SEGURANÇA consiste na prestação dos seguintes serviços, Serviços de monitoramento de ataques cibernéticos, Serviços de resposta a incidentes de segurança, Serviços de Segurança para Sistemas Críticos, Serviços de testes de invasão, assim definidas:

2.3 REQUISITOS GERAIS DOS SERVIÇOS

Os requisitos gerais dos serviços, define os requisitos obrigatórios para todos os serviços que compõem o objeto SERVIÇOS GERENCIADOS DE SEGURANÇA.

2.3.1 CANAIS DE COMUNICAÇÃO

Para abertura de solicitações a CONTRATADA deverá disponibilizar três tipos de canais de comunicação, a saber:

item	Grupo de Tecnologia	Classificação
1	Linha de telefonia gratuita (0800).	Tipo 1
2	E-mail com domínio registrado e de propriedade da CONTRATADA.	Tipo 2
3	Sistema de ITSM do inglês <i>Information Technology Service Management</i> (Gerenciamento de Serviços de TI).	Tipo 3

TABELA 1 - TIPOS DE CANAIS DE COMUNICAÇÃO

- 2.3.1.1. Independente do canal de comunicação utilizado pelo CONTRATANTE, as solicitações devem ser convergidas, atualizadas, resolvidas e concentradas em um único sistema de ITSM do inglês *Information Technology Service Management* (Gerenciamento de Serviços de TI). Ou seja, imaginando que o CONTRATANTE realize a abertura de uma nova solicitação de serviço via linha telefônica gratuita, no segundo que segue a sua solicitação, a mesma deve constar no sistema de ITSM, assim também deve se proceder com a utilização do canal de comunicação do tipo 2: via e-mail.
- 2.3.1.2. Sobre o canal de comunicação do tipo 1: via linha telefonia gratuita (0800), tais ligações obrigatoriamente devem ser atendidas e/ou recepcionadas por uma interface humana, não sendo permitido utilização de URA (Unidade de Resposta Audível), e/ou qualquer usufruto de atendimento eletrônico.
- 2.3.1.3. Para requisições de serviço de severidade alta, ou seja, que exige uma velocidade de comunicação e atendimento maior, a CONTRATADA deverá disponibilizar ao menos 1 (um) aparelho telefônico do tipo VOIP, a ser instalado nas dependências do CONTRATANTE, em local a ser indicado pelo CONTRATANTE, que ao ser utilizado deve de forma automática fazer contato com a central de serviço da CONTRATADA.

- 2.3.1.4. Para um eventual cenário de crise, ou seja, onde o negócio fim do CONTRATANTE estar sendo fortemente afetado por um problema envolvendo a segurança da informação, a CONTRATADA deverá disponibilizar uma sala de videoconferência virtual de sua propriedade, onde a qualquer tempo poderá ser utilizada para reuniões emergenciais para tratamento de crises.
- 2.3.1.5. Tal sala deve está disponível via internet e seu acesso deve obrigatoriamente ser criptografado, utilizando protocolo SSL do inglês Secure Socket Layer, com certificado digital emitido em nome da CONTRATADA. A CONTRATADA também deve garantir que os protocolos de comunicação, utilizados pela sala de videoconferência deve ser criptografado.
- 2.3.1.6. A sala virtual ainda deve ter capacidade para até 10 (dez) pessoas do CONTRATANTE simultaneamente, e afim de evitar eventuais perdas de tempo em momento de crise, a sala deve está acessível a qualquer tempo, não sendo criada apenas no momento da crise.

2.3.2 HORÁRIO DE ATENDIMENTO.

- 2.3.2.1. Os SERVIÇOS GERENCIADOS DE SEGURANÇA, devem obrigatoriamente serem executados, ofertados, e estarem acessíveis ao CONTRATANTE em regime de 24 (vinte quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, durante todo o período de vigência do contrato.

2.3.3 GESTÃO DE CATALOGO DE SERVIÇO DO AMBIENTE DE SEGURANÇA DA INFORMAÇÃO.

- 2.3.3.1 Afim de fornecer uma única fonte de informação sobre os SERVIÇOS GERENCIADOS DE SEGURANÇA, disponíveis para cada grupo de tecnologia dos itens de configuração do parque de segurança da informação do CONTRATANTE, se definiu previamente um catálogo de serviços, o qual obrigatoriamente a CONTRATADA deverá ser capaz de entregar. Tal definição pode ser consultada através do anexo II do presente termo de referência.
- 2.3.3.2 É de responsabilidade da CONTRATADA manter, atualizar, revisar, os serviços disponíveis para cada grupo de serviço. As responsabilidades do CONTRATANTE estão relacionadas a aprovação de um novo serviço, ou a aposentadoria de um ou mais serviços existentes.
- 2.3.3.3 O catálogo de serviço deverá ser mantido e administrado através do sistema de ITSM de responsabilidade da CONTRATADA, estando este disponível de forma on line para o CONTRATANTE, onde mesmo poderá consultar a qualquer tempo os serviços disponíveis. Este sistema deve ser o mesmo descrito no tópico do presente termo de referência, e obviamente deve seguir os mesmos requisitos técnicos supracitados.
- 2.3.3.4 Apesar de já existir uma definição prévia dos serviços a serem ofertados pela CONTRATADA, através do catálogo de serviço do anexo II do presente termo de referência, o CONTRATANTE a qualquer tempo poderá solicitar a inclusão de

novos serviços, ou a retirada de um serviço, porém limitando-se as soluções listadas no tópico AMBIENTE TECNOLÓGICO DO CONTRATANTE (HARDWARE E SOFTWARE) do presente termo de referência.

- 2.3.3.5 Também se espera que tais revisões de continuidade de um serviço no catálogo de serviços, seja sugerido por parte da CONTRATADA durante a execução do contrato, todavia não é de responsabilidade da CONTRATADA a retirada ou inclusão de um serviço, cabendo apenas ao CONTRATANTE tal ação.
- 2.3.3.6 O catálogo de serviços descritos no anexo II do presente termo, estar limitado aos itens de configuração, bem como seus grupos de tecnologia, descritos no tópico AMBIENTE TECNOLÓGICO DO CONTRATANTE (HARDWARE E SOFTWARE) do presente termo, inclusões de serviços podem acontecer a qualquer tempo, porém se limitando a tais itens de configuração.

2.3.4 MODALIDADE DE ATENDIMENTO.

- 2.3.4.1 2.3.4.1. A modalidade principal de atendimento será do tipo remota, ou seja, a ser realizada através das dependências da CONTRATADA, obrigatoriamente obedecendo os critérios estabelecidos para execução do mesmo, no presente termo de referência.
- 2.3.4.2 Eventualmente o CONTRATANTE poderá solicitar uma visita técnica, para que um atendimento qualquer possa ser realizado e/ou acompanhado, em suas dependências físicas, bem como também em suas regionais.
- 2.3.4.3 Os atendimentos referente ao objeto contratado denominado SERVIÇOS GERENCIADOS DE SEGURANÇA é ilimitado durante o período de vigência do contrato, ou seja, não existe limite para quantidade de horas, e/ou quantidade de atendimentos realizados, com exceção do item **Erro! Fonte de referência não encontrada.**, que deverá ser solicitado sobre demanda em regime de banco de horas.

2.3.5 ACESSIBILIDADE E CONFIDENCIALIDADE.

- 2.3.5.1 Para garantir a qualidade e disponibilidade dos serviços remoto, deverá entre o CONTRATANTE e os 2 (dois) CSOC da CONTRATADA, haver dois tipos de conexões digitais de tipo distintos, sendo uma do tipo internet e outra do tipo MPLS do inglês Multi-Protocol Label Switching.
- 2.3.5.2 Ambos as conexões digitais devem ter velocidade de upload e download mínima de 10 (dez) Mbps, ser contratadas de operadoras e rotas distintas, e devem ser utilizadas única e exclusivamente para prestação do SERVIÇOS GERENCIADOS DE SEGURANÇA do CONTRATANTE.
- 2.3.5.3 Especificamente para o tipo de conexão digital internet, necessariamente precisará ter IP dedicado, e não serão aceitos contratos com links xDSL (executada a tecnologia HDSL). Também afim de garantir a disponibilidade da conexão, deverá a contratar garantir que tal conexão esteja protegida contra ataques de DDoS do inglês Distributed Denial of Service.

- 2.3.5.4 Em qualquer que seja o tipo de conexão, será de responsabilidade e propriedade da CONTRATADA a contratação junto as devidas operadoras, bem como seus devidos custos durante todo período de vigência do contrato.
- 2.3.5.5 Afim de garantir a segurança do tráfego bidirecional entre o CONTRATANTE e os CSOC da CONTRATADA, ambas as conexões (Internet e MPLS) devem ser criptografada. Ou seja, a CONTRATADA deverá estabelecer duas VPN's do inglês Virtual private network, do tipo site to site, para cada CSOC.
- 2.3.5.6 Será de responsabilidade e propriedade da CONTRATADA os equipamentos e/ou soluções para estabelecer as VPN's, caberá ao CONTRATANTE apenas a disponibilidade de infraestrutura física no seu Data Center, infraestrutura física leia-se: energia elétrica, espaço no rack, climatização adequada, e sistemas de combate a incêndio. Tais equipamentos e/ou soluções devem possuir contratos de garantia junto ao seu respectivo fabricante, com suporte em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano.
- 2.3.5.7 A CONTRATADA deve assinar e entregar ao CONTRATANTE na data de reunião de início do contrato termo de confidencialidade e sigilo, conforme modelo contido no Anexo V – Termo de Confidencialidade e Sigilo. Esse documento estabelece as condições para a prestação dos serviços acerca do sigilo das informações custodiadas, do acesso restrito das informações aos técnicos designados no projeto e da propriedade intelectual de todos os produtos e conhecimento advindos da execução.
- 2.3.5.8 Além disso, o termo de confidencialidade e sigilo deve ser reconhecido e assinado por todos os funcionários que venham executar serviços, diretamente ou indiretamente, no âmbito do contrato, sendo que o CONTRATANTE pode solicitar, a qualquer momento, a comprovação dessa obrigação. O respectivo termo deve ser entregue antes do início das atividades.
- 2.3.5.9 Por outro lado, a CONTRATADA deve revogar todas as credenciais relacionadas a soluções de responsabilidade da CONTRATADA, empregadas na prestação de serviços ao CONTRATANTE, bem como solicitar a revogação destas ao CONTRATANTE, para soluções de responsabilidade da CONTRATADA, no mesmo dia do encerramento das atividades.
- 2.3.5.10 Tais exigências visam proteger o CONTRATANTE contra o uso indevido de informações sob sua custódia por parte de profissional da CONTRATADA, assim como estão em conformidade com boas práticas de gestão e governança de TI.

2.3.6 CSOC - CYBER SECURITY OPERATIONS CENTER.

- 2.3.6.1 Os serviços gerenciados de segurança devem ser executados por meio de 2 (dois) CSOC (Cyber Security Operation Center) redundantes, próprios da CONTRATADA, sendo ambos obrigatoriamente no Brasil, de modo que a indisponibilidade de um deles não afete a prestação dos SERVIÇOS GERENCIADOS DE SEGURANÇA, e a no mínimo 500 (quinhentos) km de distância geodésica uma da outra.

2.3.6.2 Ambos os centros (CSOC) devem atender os mesmos requisitos mínimos, a saber:

- a) Utilizar sistema de gerenciamento de CFTV, que viabilizem o rastreamento de pessoas dentro do ambiente da CONTRATADA e cujas imagens possam ser recuperadas;
- b) Filmar toda a área, mantendo as imagens armazenadas pôr no mínimo 90 (noventa) dias;
- c) Efetuar registro de entrada e saída dos visitantes, com identificação individual, em todos os acessos ao CSOC;
- d) Possuir solução de monitoramento de disponibilidade e desempenho.
- e) O perímetro físico do CSOC deve ser equipado com sensor de intrusão e alarmes contra acesso indevido;
- f) Ser vigiado de forma ininterrupta por segurança física especializada e armada em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano;
- g) Ter controle de acesso físico com pelo menos 2 (dois) dos seguintes fatores de autenticação, a saber: cartão de identificação magnético, biometria de leitura de digital ou análise de retina;
- h) Funcionar em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano;
- i) Possuir registro de entrada e saída de pessoas mantidos por pelo menos 90 dias.
- j) Possuir sistemas redundantes para armazenamento de dados e alimentação de energia.
- k) Possuir estrutura de armazenamento de dados que permita a manutenção dos registros dos eventos relacionados aos serviços contratados por, no mínimo, o prazo do contrato.
- l) Ser configurado de forma que a falha de um dos equipamentos isoladamente NÃO interrompa a prestação dos serviços;
- m) Ter sistema de provimento ininterrupto de energia elétrica, composto por grupo gerador e UPSs do inglês *Uninterruptible Power Supply*, para garantir a transição entre o fornecimento normal da energia e o grupo gerador;
- n) Ter componentes de segurança necessários para garantir a preservação dos dados em casos de incêndio e execução de plano de recuperação de catástrofes;
- o) Não possuir campo físico visual externo das suas instalações, afim de garantir que as informações exibidas em monitores estejam inacessíveis a leituras e a capturas externas desautorizadas;
- p) Possuir ambiente dedicado único e exclusivamente para laboratório, onde seja possível reproduzir os incidentes e problemas do CONTRATANTE, sem que haja impacto na operação do CSOC e/ou do próprio CONTRATANTE;
- q) Deverá possuir processos implementados que garantam a segurança das normas ABNT NBR ISO/IEC 27001. Tal certificação deverá garantir controles rígidos e auditáveis de acesso físico e lógico as informações monitoramento;

2.3.6.3 Ao menos 1 (um) CSOC da CONTRATADA deverá possuir as características das certificações listadas na tabela abaixo. Tais características garante que a CONTRATADA segue os principais controles de segurança da informação, bem como também possui processos para tratamento de incidente e problemas bem estabelecidos, além de boa qualidade de atendimento e interface com o cliente.

item	Certificações
1	ABNT NBR ISO/IEC 27001
2	ABNT NBR ISO/IEC 20001
3	ABNT NBR ISO/IEC 9001

TABELA 2 - CERTIFICAÇÕES DO CSOC

2.3.6.4 Além disso, afim de garantir a disponibilidade das ferramentas e soluções utilizadas para a execução do objeto do presente termo de referência, ambos os CSOC devem utilizar as infraestruturas de Data Centers distintos, ou seja, dois ou mais datacenters, sendo ao menos 1 (um) deles de propriedade da CONTRATADA.

2.3.6.5 Ambas infraestruturas de datacenter podem estar situadas fora dos ambientes de CSOC, e devem obrigatoriamente atender aos requisitos técnicos elencados, a saber:

- a) Estrutura física dedicada e construída com a finalidade exclusiva de prestação de serviços de hospedagem de aplicações e equipamentos, de modo a garantir um ambiente seguro e controlado, ou seja, não poderá possuir instalações hidráulicas na infraestrutura do Data Center;
- b) Todos os equipamentos envolvidos na solução a ser disponibilizada deverão possuir fontes redundantes;
- c) Deverá possuir piso elevado em placas de aço com enchimento em concreto com medidas de até 600mm x 600mm com resistência mínima à carga distribuída de aproximadamente 733 kg/m² (setecentos e trinta e três quilogramas por metro quadrado);
- d) Deverá contar com eletrocalhas exclusivas para sistema elétrico e lógico, independentes entre si;
- e) Deverá possuir área de estacionamento livre e privado, com acesso seguro para desembarque e manuseio de equipamentos com vigilância armada;
- f) Deverá possuir área de desembalagem, manuseio que poderá ser utilizado, sem ônus para manutenção, adição e/ou operação;
- g) Deverá possuir guarita com segurança armada em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano. A guarita de segurança deverá estar fora do prédio de Data Center, criando-se uma barreira física ao acesso do Data Center, ter acesso a todo o sistema de CFTV, inclusive em tempo real, e detecção de intrusos em todas as cercanias onde está localizado o Data Center;
- h) Toda a área do Data Center deve ser desprovida de janelas, básculas ou quaisquer formas de acesso que não através dos controles de acesso;
- i) Garantir a disponibilidade de pessoas dedicadas, treinadas e responsáveis pela segurança de acesso ao prédio e aos equipamentos do ambiente em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano;
- j) Utilizar câmeras digitais de circuito interno de televisão, monitoradas e gerenciadas; cujas imagens possam ser posteriormente consultadas por um período mínimo de 90 (noventa) dias, viabilizando o rastreamento de pessoas dentro do ambiente;

- k) As câmeras deverão cobrir todos os ângulos do túnel frio de forma que não existam quaisquer pontos cegos. A gravação e visualização em tempo real deverá ser feita em alta-resolução e em cores, com no mínimo 10 frames por segundo, tais características são necessárias para que seja possível identificação da face daqueles que pretendem adentrar as cercanias do Prédio do Data Center;
- l) As paredes do Data Center devem ser construídas em material para contenção de chamas e possuir porta corta-fogo;
- m) Sistema de detecção e combate a incêndio com uso de sensores de fumaça e fogo, distribuídos pela área do Data Center e uso de descarga de gás, com efeito supressor de combustão ou redução de oxigênio, ecologicamente aceitável e não afetar pessoas e equipamentos energizados;
- n) Garantir a detecção precoce de gases no ambiente incluindo a área situada sob o piso elevado utilizando detector VESDA, com sistema integrado de alarme monitorado e acompanhado em regime 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano;
- o) Possuir sistema integrado aos túneis de ventilação do Data Center, de forma que em havendo o disparo de gás, o fluxo de ar é interrompido para a área do evento garantindo a extinção do incêndio sem afetar demais áreas do Data Center;
- p) Em caso de sinistro, o disparo do gás deve ocorrer de forma automática, não havendo necessidade de intervenção humana;
- q) O sistema de detecção precoce e combate a incêndio deverá possuir contrato de manutenção contemplando visitas preventivas e testes do sistema com o fabricante do mesmo no mínimo a cada 03 (três) meses;
- r) A solução de ar condicionado deve ser integrada a solução de combate a incêndio, para que, em caso de incêndio os dutos de ventilação sejam automaticamente fechados sem necessidade de intervenção humana;
- s) Os equipamentos utilizados para prestação de serviços ao CONTRATANTE deverão estar instalados em racks que trabalhem dentro de um sistema de Túnel Frio;
- t) A climatização deverá ser composta por, no mínimo, segurança N+1 unidades evaporadoras e, no mínimo, segurança N+1 de condensadoras externas ao edifício, interligadas por tubos de cobre isolados adequadamente;
- u) A climatização não deverá fazer troca de ar atmosférico. Tanto a sala de servidores quanto a sala de refrigeração deverão ser fechadas para que variações de temperatura, umidade e outros contaminantes não afetem os equipamentos dentro do Data Center;
- v) Capacidade frigorífica variável e automática, com controle automático de refrigeração com variação de +/- 1°C;
- w) Sistema de monitoração para controle de temperatura, umidade relativa do ar e filtros contra poeira;
- x) Faixa de operação de 20 (vinte) a 25 (vinte e cinco) °C e 40% a 55% de umidade relativa do ar e variação máxima de temperatura de 5° por hora, conforme norma ANSI/TIA-942/2005;
- y) Os controladores digitais deverão ser configuráveis para realizar o revezamento entre unidades climatizadas, além de garantir o funcionamento do sistema de climatização em caso de falha, pela automação de sua redundância;

- z) Estar equipada com subestação elétrica própria e projetada para operar em média ou alta tensão, para atendimento aos requisitos de potência e alimentação elétrica adequadas e exclusivos para o Data Center;
- aa) Os sistemas devem ser equipados e protegidos por nobreaks, bancos de baterias e geradores que funcionam automaticamente no caso de queda do fornecimento comercial;
- bb) Cada nobreak deve possuir capacidade suficiente em regime N+1 para suportar todas as atividades do Data Center, incluindo as atividades previstas por este termo de referência;
- cc) Os nobreaks que atendem aos circuitos redundantes devem operar em regime standalone, de maneira que os nobreaks sejam completamente independentes entre si e sem risco de que a falha do primeiro se propague para o segundo;
- dd) Os bancos de baterias devem ser medidos mensalmente e trocados em caso de a tensão média das baterias ficar abaixo da recomendação do fabricante. As baterias devem estar dentro do prazo de validade e do tempo de vida útil recomendado pelo fabricante;
- ee) Entre a entrada da alimentação da concessionária e o último quadro de distribuição que atende ao Data Center deverão haver múltiplos sistemas de supressão de surto com a função de limitar surtos nas instalações de baixa tensão;
- ff) O Data Center deve possuir sistema de geração elétrica à diesel próprio e redundante, que mantenha o ambiente em pleno funcionamento, durante todo o período de eventual corte de energia pela concessionária;
- gg) A autonomia do sistema de geração elétrica a diesel (grupo gerador) deverá ser de no mínimo 48 (quarenta e oito) horas sem reabastecimento de combustível.
- hh) O reabastecimento deverá ser possível sem interromper o funcionamento dos geradores;
- ii) Para garantia a alta disponibilidade no sistema de geração elétrica a diesel, o Data Center deve possuir tanque reservatório de diesel, aliado a um contrato de reposição com os fornecedores de diesel. Com isto, mesmo em casos de desastres, o fornecimento de energia é continuado;
- jj) Os geradores devem ser capazes de ser acionados para proteger o Data Center automaticamente não apenas em eventos de falta de energia, mas também quando algum parâmetro da concessionária estiver fora das especificações (frequência, tensão, etc.);
- kk) No retorno da alimentação da concessionária, os grupos geradores devem ser capazes de sincronizarem sua alimentação e fazer a retirada da carga em rampa para evitar oscilações elétricas dentro do Data Center;
- ll) Os geradores e nobreaks devem possuir contrato de manutenção contemplando visitas preventivas e testes do sistema com o fabricante dos mesmos com periodicidade mínima 1(uma) vez por mês;
- mm) O edifício deve possuir sistema de aterramento tipo gaiola de Faraday com malha em cobre com espaçamento de até 60x60 cm sob a área de equipamentos eletrônicos;
- nn) O prédio da CONTRATADA deve atender a norma NBR 5410 para proteção de surto em todas as zonas.
- oo) Deve ser um sistema autônomo (AS) em relação à Internet por cadastro próprio, ou seja, possuir seus próprios blocos de IPv4, IPv6 e seu registro individual de ASN.

pp) Deverá possuir sistema autônomo (AS) integrado a, no mínimo, 2 (duas) operadoras distintas, através de protocolo de roteamento BGP FULL ROUTING.

qq) deverá possuir Solução Anti-DDoS, implementando proteção contra-ataques coordenados provenientes de múltiplos sistemas (comprometidos) e distribuídos geograficamente com o intuito de gerar indisponibilidade dos serviços da CONTRATANTE através do esgotamento dos recursos.

2.3.6.6 Seguindo os princípios e pilares básicos da segurança da informação (confiabilidade, disponibilidade e integridade), além dos requisitos técnicos exigidos para todos os Data Center utilizados pelo CSOC descritos acima, ao menos 1 (um) dos Data Centers, a qual hospedam os serviços e soluções dos CSOC, devem possuir as seguintes certificações ou normas, a saber:

item	Certificações	Descrição
1	ABNT NBR ISO/IEC 27001	Norma que especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI (Sistema de Gestão de Segurança da Informação) documentado dentro do contexto dos riscos de negócio globais da organização.
2	ABNT NBR ISO/IEC 22301	norma de gestão da continuidade de negócios especifica os requisitos para planejar, estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar continuamente um sistema de gestão documentado para se proteger, reduzir a possibilidade de ocorrência, preparar-se, responder a e recuperar-se de incidentes de interrupção quando estes ocorrerem.
3	UPTIME INSTITUTE – DESIGN	Certificação que ratifica a funcionalidade e a capacidade evidenciadas nas especificações de engenharia e de arquitetura do projeto de sua instalação de um Data Center.
4	UPTIME INSTITUTE – INSTALAÇÃO	Certificação que garante que as instalações do Data Center, foram construídas conforme o projeto, e verifica se ela é capaz de cumprir com as exigências de disponibilidade definidas.

TABELA 3 - CERTIFICAÇÕES DO DATA CENTER

2.4 SERVIÇOS DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS

Tem por objetivo o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados ao CONTRATANTE, através de correlacionamento de logs, pacotes de redes, e/ou comportamento anômalo de aplicações, serviços e infraestrutura do CONTRATANTE, que possam gerar eventos de segurança da informação, aos quais devem ser analisados, podendo estes serem transformados em um incidente de segurança da informação, obedecendo um processo cíclico e rigoroso de gestão de eventos.

2.4.1 SOBRE AS FERRAMENTAS A SEREM UTILIZADAS

2.4.1.1 Todas as ferramentas e soluções hardware e/ou software, deverão possuir os seguintes requisitos nativos, a saber:

- a) Deverá ser obrigatoriamente de propriedade da CONTRATADA, não poderá ser do tipo *open source* (software livre).
- b) Deverá ser prestado por meio de solução provida através da nuvem do fabricante ou da CONTRATADA.
- c) Devem englobar a alocação de equipamentos e/ou softwares necessários à consecução das atividades de segurança da informação e ao atendimento das especificações técnicas do objeto durante o prazo de vigência do contrato, incluindo garantia, manutenção, atualização dos produtos e monitoramento de segurança em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano;
- d) Todos os equipamentos necessários à prestação dos serviços devem ser novos e de primeiro uso. Além disso, os equipamentos e softwares não podem constar, no momento da apresentação da proposta técnica, em listas de *end-of-sale*, *end-of-support*, *end-of-life* ou similares do fabricante, ou seja, não podem ter previsão de descontinuidade de fornecimento, suporte ou vida;
- e) Os softwares ofertados devem ser instalados em sua versão mais estável e atualizada e estar cobertos por contratos de suporte e atualização de versão do fabricante durante a vigência do respectivo item de serviço. Da mesma maneira, os equipamentos fornecidos para a prestação dos serviços devem estar cobertos por contratos de garantia do fabricante;
- f) O conjunto de requisitos especificados para cada serviço pode ser atendido por meio de composição com outros equipamentos ou softwares utilizados no atendimento aos demais itens, de maneira integrada, desde que não implique alteração da topologia de rede ou na exposição de ativos a riscos de segurança da informação, em termos de integridade, confidencialidade ou disponibilidade.
- g) Todos os módulos que compõe a solução deverão se integrar de forma nativa e visando constituir um ambiente homogêneo de análise, investigação, inteligência, defesa cibernética e resposta a incidentes nos processos, incluindo má utilização dos sistemas e tentativas sequenciais de utilização suspeitas inclusive entre sistemas e plataformas diferentes;

- h) Deve possuir arquitetura de forma distribuída, possuindo no mínimo os seguintes módulos ou componentes: módulo de coleta de pacotes e logs e geração de metadados, módulo de indexação, agregação e enriquecimento dos metadados dos coletores, módulo de correlacionamento avançado de alertas e tratamento de incidentes e módulo de gerência centralizada de todos os outros módulos envolvidos;
- i) Permitir a correlação de eventos provenientes de logs e pacotes do tráfego de rede, devidamente estruturados em metadados;
- j) Deverá ter capacidade e ser licenciada para processar no mínimo todos os eventos gerados pelos ativos de segurança do ambiente tecnológico listados anteriormente;
- k) Deverá ser capaz de processar, no mínimo, Oito mil Mbps (Oito mil Megabits por segundo) de volume de tráfego de rede; Deverá possuir retenção mínima de 1 ano dos registros de eventos;
- l) Ser capaz de integrar em uma única console de visualização, dados e metadados de logs e pacotes do tráfego de rede;
- m) Permitir buscas utilizando expressões regulares e palavras-chave em todo o conteúdo dos dados e metadados capturados;
- n) Possuir compatibilidade e integração nativa com pelo menos uma solução de forense comportamental de endpoints (EDR), com intuito de complementar a visibilidade entregue e capacidade de análise de atividade maliciosa;
- o) Prover uma console e visão altamente intuitiva para realizar investigações sobre os dados;
- p) Possuir a capacidade de navegação contínua sobre os dados em formato “drill down”, sem a obrigatoriedade de realizar pesquisas avançadas;
- q) Prover uma interface extremamente intuitiva, permitindo que em até três cliques seja possível chegar a uma ação suspeita ou ataque, sem prévio conhecimento da mesma;
- r) Integrar-se nativamente com uma solução de análise forense de estações, sendo capaz de utilizar dados e indicadores de comprometimento gerados pela mesma;
- s) Permitir a criação e customização de regras, alertas, gráficos e relatórios na própria interface;
- t) Deve possuir pelo menos 150 regras pré-definidas;
- u) Deve permitir o agendamento automático e manual de relatórios, com a possibilidade de envio por e-mail;

- v) O fabricante da solução deve possuir ampla experiência em malwares, assim como possuir seu próprio centro de pesquisa e desenvolvimento e inteligência às novas ameaças;
- w) Deve ter sua base de inteligência diariamente atualizada através de alimentadores (feeds) de informação, provenientes da base de conhecimento em ameaças da própria empresa e de terceiros;
- x) Deve permitir o desenvolvimento e customização de interpretadores (parsers) utilizando linguagens XML e LUA, através de ferramenta gráfica do mesmo fabricante;
- y) Deve ser capaz de detectar em tempo real, ameaças alimentadas pelas seguintes bases de inteligência:
 - i. relatórios de ameaças e segurança;
 - ii. relatórios de botnets e centros de Comando e Controle; identificação de exploit kits;
 - iii. indicadores de ataques “zero-day”;
 - iv. indicadores de comprometimento, suspeitas e avisos Informativos; inteligência de tendências;
 - v. proxies anônimos;
 - vi. classificação de sites;
 - vii. endereços de rede TOR.
- z) Deve possuir integração nativa com módulo de análise de malware de mesmo fabricante;
- aa) O módulo de análise de malware deve permitir o uso de regras YARA;
- bb) Deve possuir integração nativa com soluções de gestão de centro de operações de segurança (Security Operations Center - SOC);
- cc) Deve permitir a criação de perfis de visualização do metadados derivados dos dados capturados;
- dd) Deve possuir mecanismo de auditoria através da geração de logs das atividades realizadas no console de gerência e investigação;
- ee) Deve permitir a visualização e análise dos dados capturados em formato gráfico de linha do tempo, construindo os gráficos com base no número de sessões, bytes ou pacotes;
- ff) Deve permitir a captura de dados de forma distribuída e toda a análise centralizada;
- gg) Deve possuir controle de acesso baseado em papéis e perfis de usuários;
- hh) Deve permitir gerar relatórios em formatos HTML, PDF e CSV;

- ii) Deve possuir um módulo para construção de relatórios customizados pelo usuário, com funcionalidade do tipo arrastar-e- colar para definição dos campos e elementos dos mesmos;
- jj) Possuir a capacidade de integração com outras soluções de segurança, por meio de envio de logs/eventos via protocolos SYSLOG e SNMP;
- kk) Permitir integração nativa com módulo opcional para detecção e análise de comportamento de malware do tipo “0- day” em endpoints (EDR), de forma aprimorar as investigações da solução;
- ll) Permitir a definição e customização de alertas, relatórios e gráficos;
- mm) Possuir integração com serviço de diretório (Active Directory) e Pluggable Authentication Module (PAM);
- nn) Disponibilizar uma API ou SDK permitindo a integração e customização com a solução;
- oo) Suportar a comunicação criptografada entre os componentes envolvidos;
- pp) Fazer uso de protocolo proprietário entre os componentes, para garantir máximo desempenho;
- qq) Deve ser projetada para possuir escalabilidade infinita;
- rr) Possuir um módulo de monitoração de desempenho e saúde dos equipamentos envolvidos;
- ss) Suportar o gerenciamento dos componentes através de uma interface de gerência central;
- tt) Possuir métricas de saúde dos equipamentos como: utilização de CPU, temperatura da CPU, utilização de memória, disco rígido, status do serviço, status das conexões;
- uu) Suportar armazenamento externo através de Direct-Attached Capacity (DAC) ou Storage Area Network (SAN);
- vv) Possuir interface de rede dedicada para a gerência da solução, podendo esta ser em 100 Mbps - FastEthernet, sendo desejável em 1Gbps Ethernet (fibra ou cobre);
- ww) Possuir interface de rede dedicada para a aquisição (captura) de dados;
- xx) Permitir o uso no mínimo das seguintes interfaces de rede: 1GbpsEthernet (copper), 1GbpsEthernet (fiber - SFP LR / SR / LX / LH), 10GbpsEthernet (fiber - SPF+ LR / SR), 40GbpsEthernet (fiber QSFP ou brake-out cable);

- yy) Possuir relatórios de conformidade e regulamentações pré-definidos (out-of-the-box) como BASEL II, FERPA, FFIEC, FISMA, GLBA, HIPPA, ISO27002, NERC-CIP, NISPOM, PCI e SOX;
- zz) Utilizar sistema operacional baseado em Linux;
- aaa) Deverá segregar a visualização de relatórios apenas para usuários com a devida permissão;
- bbb) Possuir a criação de relatórios utilizando qualquer informação armazenada no sistema;
- ccc) Suportar a integração nativa com sistemas de GRC (Governance, Risk e Compliance), possibilitando a integração de dashboards entre as soluções e provendo contexto de governança a um incidente gerado pela solução proposta;
- ddd) Possuir a funcionalidade para resolução de endereços IP, como localização da cidade, país e organização das conexões;
- eee) Possuir a capacidade de exportar e importar arquivos no formato packet capture (pcap);
- fff) Permitir a visualização das sessões nos seguintes formatos: metadado, texto, hexadecimal, pacotes, reconstrução Web (HTTP), reconstrução e-mail (SMTP) e arquivos (binários);
- ggg) Suportar a análise de dados na camada de aplicação (modelo OSI) a partir de entidades como usuários, e-mail, endereço, arquivos e ações;
- hhh) Suportar a aplicação de filtros na camada de rede e de aplicação, no mínimo MAC, IP, usuário e palavras-chave;
- iii) A solução deve suportar a decifração de tráfego SSL, por meio do uso de appliances físicos dedicados a este propósito;
- jjj) Suportar a geração de hash (MD5 e SHA1) para verificação de integridade dos arquivos extraídos a partir do tráfego de rede capturado;
- kkk) Deve possuir a capacidade de extração de metadados do tráfego de dados capturado, com reconhecimento nativo de no mínimo os seguintes protocolos e aplicações: FTP, SCP, HTTP, HTTPS, IMAP, IRC, MAIL (RFC822), NETBIOS, POP3, RDP, SIP, SMB, SMIME, SMTP, SNMP, SSH, TELNET, TNS, DNS, TORRENT.
- lll) Possuir a capacidade de criação de interpretadores (parsers) para protocolos e aplicações proprietárias e/ou não conhecidas;
- mmm) Possuir a capacidade de identificação de protocolo pelo conteúdo das sessões, independente da porta utilizada de comunicação;
- nnn) Pertinir isolar sessões de tráfegos, com identificação de conteúdo (payload) de origem e destino, para os protocolos ICMP, TCP e UDP;

- ooo) Permitir a extração dos arquivos presentes no tráfego de rede capturado no formato compactado .zip;
- ppp) Alertar em tempo real sobre tráfego coincidente com assinaturas pré-definidas e permitir a visualização da sessão em que a assinatura ocorreu, assim como a exportação da sessão para o formato .pcap;
- qqq) Possuir ferramenta para administração centralizada dos módulos de captura do tráfego de rede, permitindo a replicação de parâmetros de configuração entre os dispositivos a partir de uma única fonte;
- rrr) Deve permitir a criação customizada de interpretadores (parsers) através de linguagem XML para identificação de protocolos de rede específicos;
- sss) Ser capaz de analisar tráfego IPv4 e IPv6;
- ttt) Permitir a customização de um interpretador de busca, cuja função é analisar todas as sessões de rede em busca de palavras chaves ou sentenças;
- uuu) Funcionar somente em modo passivo sem adicionar latência à rede durante a monitoração passiva;
- vvv) Possuir discos de alto desempenho como Solid-State Drives (SSDs) nos servidores físicos que realizam a indexação de metadados;
- www) Armazenar todos os pacotes de forma segura;
- xxx) Permitir nativamente, a análise automatizada e ampla de malwares e suas atividades de rede;
- yyy) Permitir a captura e análise de características suspeitas em arquivos de conteúdo executável na rede em tempo real; A solução deve possuir um mecanismo de pontuação de risco no momento da análise de malwares;
- zzz) Permitir plena integração com outras tecnologias de análise em sandbox, tanto em equipamento físico ou SaaS;
- aaaa) Possuir painel (dashboard) configurável que permita a rápida visualização do status da segurança e acesso granular a sessão reconstruída equivalente ao tráfego que gerou o alerta;
- bbbb) Possuir a capacidade de exibir visualmente os objetos trafegados pela rede sem a necessidade de manipular os dados diretamente na console ou banco de dados;
- cccc) Permitir que a partir de uma informação existente em um relatório, se verifique o tráfego de rede que a gerou através de recurso de “drill-down”;
- dddd) Ser capaz de identificar a troca de extensão de arquivos (arquivo .exe enviado como .jpg);

- eeee) Possuir um módulo de análise avançada de eventos, podendo comparar metadados e correlacionar eventos em uma base histórica;
- ffff) Permitir o processamento de eventos/logs, apenas com a adição de componentes para tal finalidade, mantendo a taxonomia dos metadados;
- gggg) Ser capaz de coletar e armazenar todos os logs de ativos de rede e dispositivos que são recebidos em sua interface de rede, gravando-os em formato original para posterior uso em fins forenses;
- hhhh) Ser capaz de coletar os logs dos ativos de rede e dispositivos de forma não intrusiva, sem a instalação de agentes;
- iiii) Suportar a criação de interpretadores (parsers) para os logs não suportados nativamente através de linguagem XML e LUA;
- jjjj) Suportar a criação de interpretadores (parsers) customizados para no mínimo 20 sistemas proprietários das proponentes;
- kkkk) Suportar de forma nativa os logs de pelo menos 300 dispositivos diferentes de diversos fabricantes;
- llll) Possuir a capacidade de geração de alertas sobre qualquer dado ou comportamento desejado e permitir o envio deste alerta a plataformas externas como SIEM ou SYSLOG;
- mmmm) Possuir capacidade de coletar logs de sistemas operacionais Windows, Linux, Unix e FreeBSD;
- nnnn) Ser capaz de coletar logs de firewalls, antivírus, IDSs, proxies, servidores DNS, load balancers e demais dispositivos de segurança;
- oooo) Ser capaz de coletar logs e eventos de quaisquer dispositivos e aplicações IP que suportem nativamente os protocolos: SYSLOG, SYSLOG-NG, SNMP, Microsoft Windows Event Logging API, Microsoft Windows Remote Management, CheckPoint LEA, arquivos de logs recebido via FTP, arquivos de logs formatados por delimitadores, ODBC, CISCO e CISCO Security Device Event Exchange (SDEE);
- pppp) Utilizar formatos de logs/eventos através de formatos nativos de cada fabricante do dispositivo, sem utilizar um tipo de formato comum definido pelo proponente da solução;
- qqqq) Deve exigir a adição de agentes ou software nos dispositivos monitorados, exceto caso o dispositivo a ser monitorado não disponibilize nenhum meio nativo de envio de logs citado no item anterior;
- rrrr) Deve coletar e armazenar logs/eventos dos dispositivos sem realizar normalização no momento da coleta;
- ssss) Deve fazer uso de sistema de bancos de dados relacional por questão de desempenho, normalização e DBAs requeridos por esses sistemas;

- tttt) Permitir que os logs/eventos dos dispositivos da CONTRATANTE sejam enriquecidos com informações de classificação de risco;
- uuuu) Permitir o correlacionamento de logs/eventos próximo ao tempo real;
- vvvv) Notificar através de alertas, comportamentos anômalos baseados em múltiplos eventos que ocorrerem em um determinado período de tempo;
- wwwv) Possuir um painel de controle (Dashboard), onde através de simples “drill-down” possa ver o log/evento coletado; A solução deve fornecer painel de controle (Dashboard) que constantemente mostre o status do ambiente de correlação de eventos; A solução deve ser capaz de notificar o administrador caso algum dispositivo monitorado pare de enviar eventos;
- xxxx) Permitir que o administrador possa filtrar logs/eventos ao gerar relatórios;
- yyyy) Oferecer uma plataforma unificada, acessível via browser WEB para realizar investigações, gestão de incidentes, gestão de alertas, gestão de relatórios, administração dos componentes e gestão de inteligência externa;
- zzzz) Permitir que os relatórios sejam executados em periodicidade diária, semanal, mensal ou em ocasiões específicas de forma automática;
- aaaaa) Possuir a capacidade de análise avançada de eventos em tempo real através de regras de correlacionamento e eventos complexos em dados correlacionados através da linguagem EPL (Event Processing Language), com mecanismo de versão igual superior à 5.3;
- bbbbbb) Suportar nativamente a coleta de NetFlow, sendo capaz de capturar, analisar e correlacionar de forma contínua até 25000 fluxos por segundo na versão 5 e 15000 fluxos por segundo na versão 9;
- ccccc) Deve detectar de forma nativa ataques do tipo NetFlow Synflood na coleta de Netflows;
- ddddd) Ter a habilidade de receber logs/eventos oriundos de um relay de syslog;
- eeeeee) Suportar o recebimento de eventos no formato Common Event Format (CEF);
- fffff) Possuir serviço de monitoração de estado de recebimento e/ou processamento de logs/eventos;
- ggggg) Possuir procedimento de Backup & Restore para um sistema de armazenamento de longo prazo, implementando o conceito de arquivador.
- hhhhh) Suportar de forma nativa e automática o armazenamento em camadas, com as seguintes funcionalidades: HOT (dados presentes em sistemas como DACs e SANs), WARM (dados presentes em sistemas como

NAS para pesquisa, execução de relatórios, exportação de dados) e COLD (dados presentes em sistemas de armazenamento off-line para possível restauração em WARM);

iiii) Suportar nos sistemas de armazenamento de longo prazo, pelo menos 3 algoritmos de compressão: gzip, bzip2 e lzma;

jjjj) Permitir a agregação em grupos de instâncias dos vários sistemas de armazenamento de longo prazo;

kkkk) Permitir a exportação de logs/eventos armazenados nos formatos texto, XML, JSON, CSV;

llll) Possuir um módulo específico para tratar dados arquivados e/ou recuperados;

mmmm) Ser baseada em plataforma WEB, com acesso via browser padrão de mercado, sem a necessidade de instalação de aplicações cliente nas estações dos analistas responsáveis pela resposta aos incidentes;

nnnn) Permitir a criação e acompanhamento de Incidentes de Segurança, de forma manual ou automática, com no mínimo as seguintes características:

- i. Sumário do incidente, incluindo título, sumário e detalhes. Também deverá incluir o status do incidente, incluindo data de criação, de modificação, de fechamento, tempo em que o chamado está aberto, número de alertas agregados, prioridade e analistas envolvidos;
- ii. Classificação inicial da ameaça, incluindo categoria, origem (interna/externa), possibilidade de modificação manual da prioridade e justificativa, além de informações específicas para subsidiar o relatório de incidentes e possibilidade de inclusão de documentação adicional através da anexação de arquivos;
- iii. Possibilidade de manter o histórico de atividades realizadas pelos analistas, tais como criação de registros, atualização de campos, etc;
- iv. Permitir agregar vários alertas em um único incidente. Esta agregação de alertas deverá permitir a visualização rápida de, no mínimo, os seguintes campos: horário do alerta, nome, prioridade e aspectos comportamentais;
- v. Definição das tarefas a serem executadas. A plataforma deverá conter uma biblioteca de procedimentos de resposta já existente;
- vi. Permitir inserir comentários dos analistas no incidente, de tal forma a possibilitar o registro de todas as atividades de análise; Permitir inserir análise forense de host e rede como um complemento da análise do incidente;
- vii. Permitir registrar os resultados de um Incidente incluindo sua confirmação, categoria de ataque, identificação de técnicas utilizadas,

detalhes sobre o alvo dos ataques e eficácia dos controles de detecção, prevenção e investigação;

- viii. Permitir análise comportamental para detecção automática de incidentes relacionados às atividades de Comando e Controle (C2);
- ix. Permitir detecção de Movimentos Laterais para identificação de atividades de login suspeitas em ambientes Windows e Linux; A solução deve possuir tecnologia de análise comportamental (UBA), baseado em técnicas de "machine learning" e análises estatísticas para a monitoração de segurança, gerando índices de riscos para eventos e entidades mapeadas;
- ooooo) Exibir a data e hora do último login no rodapé da interface, de forma garantir que a credencial não esteja sendo compartilhada;
- ppppp) Permitir o processamento de informações estruturadas de ameaças STIXTM ("Structured Threat Information eXpression");
- qqqqq) Possuir um ambiente de construção de regras que ofereça um mecanismo de testes (debug), visando à redução de erros de lógica e sintaxe;
- rrrrr) Permitir o ajuste de sessões concorrentes na interface de gerência;
- sssss) Permitir a customização de perfis de visualização de metadados de acordo com o objetivo da investigação (ex.: Análise Web, Análise e-mail, Análise de Arquivos, etc.);
- ttttt) Possuir um menu de contexto na interface de investigações, de forma visualizar instantaneamente se endereços foram encontrados em Alertas, Incidentes ou Listas.

2.4.2 PROCESSO DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS

- 2.4.2.1 Afim de balizar todo o processo de monitoramento de ataques cibernéticos do CONTRATANTE, e influenciado pelos principais frameworks de boas praticas de serviços de segurança da informação, foi arquitetado o processo que será descrito nos parágrafos que seguem, o qual obrigatoriamente a CONTRATADA deve seguir *ipsis litteris*.
- 2.4.2.2 É sabido que para o sucesso de um monitoramento de ataques cibernético, a primeira definição se deve a que tipo de ocorrência de eventos de segurança, se deseja detectar e tomar algum tipo de ação, logo será de responsabilidade da CONTRATADA como primeiro passo deste processo, a definição de linha de base de eventos monitorados.
- 2.4.2.3 Tal definição de linha de base de eventos de segurança monitorados, não deve ser tomada de forma unilateral pela CONTRATADA, o CONTRATANTE deverá participar ativamente no processo de construção de forma consultiva, porém se

ratifica que é de responsabilidade da CONTRATADA a definição e colocar em operação tal linha de base.

- 2.4.2.4 Espera-se que a linha de base de eventos de segurança monitorados, seja revista de forma mensal, contudo não se limitando a este tempo, pois todos os dias novos ataques são projetados no mundo, e se espera que a CONTRATADA tome ciência deste ataques, e por sua vez atualize a linha de base, para que em um cenário onde estes novos ataques seja direcionados ao CONTRATANTE, sejam detectados através dos serviços em questão.
- 2.4.2.5 O produto de um evento é a correlação dos insumos: logs e pacotes de rede, gerados pelos itens de configurações do parque do CONTRATANTE. Uma vez definido a linha de base de eventos, será também de responsabilidade da CONTRATADA avaliar se todos os insumos para a correta geração do evento, estão sendo enviados corretamente para a ferramenta definida no tópico SOBRE AS FERRAMENTAS A SEREM UTILIZADAS.
- 2.4.2.6 Caso a CONTRATADA identifique a ausência dos insumos (logs e pacotes de rede) a ser gerado por um item de configuração, será de responsabilidade da CONTRATADA a correção e/ou habilitação de tal insumo dos itens de configuração descritos no tópico AMBIENTE TECNOLÓGICO DO CONTRATANTE (HARDWARE E SOFTWARE). Caso o item de configuração não pertencer ao objeto contratado, porém necessário para a correta geração do evento, deverá a CONTRATADA solicitar ao CONTRATANTE a correção e/ou habilitação de tal insumo no item de configuração em questão.
- 2.4.2.7 Dar-se-á então o passo de classificação do evento, também de responsabilidade da CONTRATADA. O grupo de monitoramento de ataques da CONTRATADA deve focar as ações nos eventos que são significativos, logo tal grupo deve analisar todos os eventos apresentados, classificando-os nos seguintes grupos, a saber:
- a) Eventos de Informação: Estes eventos não requerem qualquer ação. São usados para fazer verificação de funcionalidade dos itens de configuração de segurança. Ou seja, tem por objetivo puro e simples, identificar se as ferramentas e soluções, estão funcionando dentro do esperado. Estes eventos são também úteis para gerar estatísticas como por exemplo, *porcentagem de hosts com a última vacina de antivírus do dia*.
 - b) Eventos de Aviso: Este grupo de eventos deve ser utilizado, quando existe algum comportamento anômalo se comparado a linha de base de operação padrão do ambiente (serviço, tráfego e/ou solução), porém ainda não gerou algum tipo de impacto ao ambiente (serviço, tráfego e/ou solução) do CONTRATANTE, como por exemplo fictício: *É esperado que exista 1000 (mil) ataques do tipo port scan bloqueados pelo firewall, porém na última hora este número passou para 10000 (dez mil) ataques, todavia o firewall ainda continua bloqueando sem que haja degradação da performance do ambiente (serviço, tráfego e/ou solução)*.
 - c) Eventos de Exceção: Estes eventos são aqueles que sugere que os pilares de segurança da informação (confidencialidade, integridade e confidencialidade), foram impactados, como por exemplo: *Uma infecção gerada por um malware do tipo ransomware, onde a mesma não tenha sido bloqueada pela solução de antivírus do CONTRATANTE*. Este é o único tipo

de evento que pode iniciar o processo de resposta a incidente de segurança, descrito no tópico PROCESSO DE RESPOSTA A INCIDENTE DE SEGURANÇA DA INFORMAÇÃO. do presente termo de referência.

2.4.2.8 Uma vez classificado o evento se inicia o passo de resposta ao mesmo, que também é de responsabilidade da CONTRATADA. As respostas são baseadas nos grupos de classificação de eventos, a saber:

- a) Para eventos do tipo Informação, não é requerido qualquer tipo de ação, porém como já mencionado no presente termo de referência, tais eventos são utilizados para verificação do perfeito funcionamento das soluções de segurança, portanto se espera que a CONTRATADA os utilize para tal.
- b) Para eventos do tipo Aviso, deve existir a garantia por parte da CONTRATADA, que uma interface humana, ou seja, uma analista que pertence ao grupo de monitoramento de ataques, esteja validando se tal evento pode se transformar em um evento do tipo exceção, e obviamente tomando as ações cabíveis para identificar a causar raiz da mudança de comportamento do ambiente.
- c) Para eventos do tipo Exceção, deverá a CONTRATADA transformar tal evento em um incidente de segurança, realizando, portanto, a abertura do mesmo na ferramenta de incidente de segurança da informação, definida no PROCESSO DE RESPOSTA A INCIDENTE DE SEGURANÇA DA INFORMAÇÃO, descrito no presente termo de referência. Após a abertura do incidente de segurança obedecendo os critérios estabelecidos para tal, se encerra a participação do grupo de monitoramento de ataques.

2.4.2.9 Como ultimo passo do processo, a CONTRATADA deve encerrar os eventos após as devidas ações tomadas, conforme definido no paragrafo acima. Eventos podem ter apenas dois tipos de status “aberto” ou “encerrado”, ou seja, após o correto tratamento o evento deverá ter seu status alterado na ferramenta de “aberto” para “encerrado”.

2.4.2.10 Importante ressaltar que todo processo de tratamento do evento, independente de qual fase e/ou status, deve ser registrado. Também é responsabilidade da CONTRATADA a segurança dos eventos, e fica expressamente proibido a remoção de qualquer evento, independente de sua classificação e fase de tratamento.

2.4.3 GRUPO TÉCNICO DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS

2.4.3.1 Através do seus 2 (dois) CSOC do inglês Cyber Security Operations Center definidos no tópico CSOC - CYBER SECURITY OPERATIONS CENTER., a CONTRATADA deverá manter uma torre de operação denominada GRUPO DE MONITORAMENTO DE ATAQUES, com objetivo e foco de trabalhar no processo de monitoramento de ataques cibernéticos.

2.4.3.2 Este grupo deverá ser exclusivo para trabalhar no serviço em questão, não podem os profissionais pertencentes a este grupo serem compartilhados e/ou atuarem, com os demais serviços descritos no objeto do presente termo de referência.

- 2.4.3.3 Todos os profissionais que integram GRUPO DE MONITORAMENTO DE ATAQUES, devem obrigatoriamente compor o quadro de colaboradores da CONTRATADA em regime de trabalho CLT (Consolidação das Leis do Trabalho), não havendo possibilidade a terceirização ou subcontratação de tal serviço.
- 2.4.3.4 Deverá ser de responsabilidade da CONTRATADA dimensionar o numero de profissionais adequado para entrega de tal serviço, sem que haja impacto no acordo de nível de serviço estabelecido no tópico ACORDO DE NÍVEIS DE SERVIÇO do presente termo de referência.
- 2.4.3.5 Afim de garantir que os profissionais envolvidos têm conhecimento e habilidade, para executar o processo monitoramento de ataques cibernéticos do CONTRATANTE, a CONTRATADA obrigatoriamente deverá compor o GRUPO DE MONITORAMENTO DE ATAQUES, com ao menos 1 (um) perfil de cada que segue descrito abaixo:

Perfis	Certificações	Descrição
Analista de Segurança I	CompTIA Security+	4. Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); 5. 6. Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. 7. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.
Analista de Segurança II	ComTIA Cybersecurity Analyst (CySA+)	9. Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); 10. 11. Conhecimento avançado em

		segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. 12. 13. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação
Analista de Segurança III	- Certified Ethical Hacker - Linux LPIC 2 - Linux LPIC 3	14. Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); 15. 16. Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. 17. 18. Experiência comprovada de no mínimo 5 (cinco) anos em segurança da informação

TABELA 8 - CERTIFICAÇÕES [GRUPO DE MONITORAMENTO DE ATAQUES]

2.4.3.6 Não existe restrição ou limite para acúmulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos no GRUPO DE MONITORAMENTO DE ATAQUES, porém conforme já fora mencionado no presente termo de referência, este(s) deve(m) compor único e exclusivamente o time denominado GRUPO DE MONITORAMENTO DE ATAQUES.

2.4.3.7 No momento da assinatura do contrato será exigido da CONTRATADA, as seguintes documentações do(s) profissionais que participarão do GRUPO DE MONITORAMENTO DE ATAQUES, os quais devem comprovar as exigências e obrigações descritas no presente termo de referência: carteira de trabalho devidamente assinada pela CONTRATADA, curriculum vitae para comprovação de habilidades, e as devidas certificações técnicas para comprovação do conhecimento.

2.4.4 ENTREGAS A SEREM REALIZADAS

2.4.4.1 Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, o CONTRATANTE definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue de

forma on line e em tempo de execução, através do portal de segurança descrito através do anexo III do presente termo de referência, a saber:

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Quantitativo de eventos correlacionados	Soma de eventos correlacionados	Eventos correlacionados	Eventos correlacionados	Número total de eventos correlacionados
Quantitativo de pacotes correlacionados	Soma de pacotes correlacionados	pacotes correlacionados	pacotes correlacionados	Número total de pacotes correlacionados
Quantitativo de incidentes abertos	Soma de incidentes abertos	Incidentes abertos	Incidentes	Número total de incidentes abertos
Quantitativo de solicitações por grupo de tecnologia	Soma de solicitações relacionadas aos grupos de tecnologia	Solicitações relacionadas aos grupos de tecnologia	Solicitações	Número total de solicitações relacionadas por grupo de tecnologia
Quantitativo de regras de correlacionamento	Soma do número de regras de correlacionamento	Regras de correlacionamento	Regras de correlacionamento	Número total de regras de correlacionamento
TOP 10 – Regras de correlacionamento	Soma do número de eventos/pacotes correlacionados por regra de correlacionamento	Eventos e pacotes correlacionados	Regra de correlacionamento	TOP 10 do número de eventos correlacionados por regra de correlacionamento
TOP 10 – IP de destino de regras de correlacionamento	Soma do número de eventos correlacionados por IP de destino	Eventos e pacotes correlacionados por IP de destino	IP de destino	TOP do número de eventos correlacionados por IP de destino
TOP 10 – Regras de correlacionamento por país de origem	Soma do número de eventos correlacionados por país de origem	Eventos e pacotes correlacionados por país de origem	País de origem	TOP do número de eventos correlacionados por país de origem
TOP 10 – Tipos de ataques	Soma do número de ataques correlacionados por tipo de ataque	Eventos e pacotes correlacionados por ataque	ataques	TOP 10 por tipo de ataque

TABELA 9 - INDICADORES ESTRATÉGICOS DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS

2.4.4.2 Tais relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços prestados e com uma das seguintes certificações: CISSP (Certified Information Systems

Security Professional), CISM (Certified Information Security Manager, CIA (Certified Intrusion Analyst), GSEC (GIAC Security Essentials), GCIH (GIAC Incident Handler) ou GMON (GIAC Continuous Monitoring), conforme condições expostas no tópico QUALIFICAÇÃO TÉCNICA DOS PROFISSIONAIS DA EMPRESA:. Nesse contexto, o profissional deve apresentá-lo de forma presencial nas dependências do CONTRATANTE ou de forma virtual, por meio de solução de videoconferência.

2.5 SERVIÇOS DE RESPOSTA A INCIDENTES DE SEGURANÇA

Tem por objetivo, analisar, remediar, conter e documentar os eventos de segurança da informação, que após analisados se descobriu que de fato era um ataque iminente ao CONTRATANTE, e foram transformados em um incidente de segurança da informação. Tal serviço deverá ser executado através de um CSOC do inglês *Cyber Security Operations Center*, obedecendo os principais frameworks de resposta a incidente de segurança da informação, e boas praticas de mercado já conhecidas.

2.5.1 SOBRE AS FERRAMENTAS A SEREM UTILIZADAS

2.5.1.1 Todas as ferramentas e soluções hardware e/ou software, deverão possuir os seguintes requisitos nativos, a saber:

- a) Permitir integração com qualquer sistema de correlação de eventos (SIEM) para recebimento de alertas e abertura automática de incidentes para tratamento via fluxo de trabalho. A plataforma contratada deverá suportar o recebimento de alertas em formato Syslog;
- b) Permitir o acesso a distintos painéis de controle, totalmente customizáveis sem a necessidade do uso de programação, através da utilização de perfis diferenciados. Dentre os perfis disponíveis, a plataforma deverá, no mínimo, contemplar os seguintes dashboards/perfis específicos:
 - i. Analista Nível 1. Responsável pela triagem inicial dos eventos;
 - ii. Analista Nível 2. Responsável pela análise mais detalhada dos eventos;
 - iii. Coordenador do SOC. Coordenador da equipe de analistas;
 - iv. Gerente do SOC. Gestor responsável por todo o SOC;
 - v. Coordenador de Brechas de Segurança. Responsável pelo acompanhamento das Brechas de Segurança que ocorreram no ambiente;
 - vi. Analistas de TI. Responsáveis pelo tratamento de tickets que envolvam ativos de TI.
- c) Permitir a criação e acompanhamento de Incidentes de Segurança, de forma manual ou automática, com no mínimo as seguintes características:
 - i. Sumário do incidente, incluindo título, sumário, detalhes, e a fonte geradora do incidente (SIEM). Também deverá incluir o status do incidente, incluindo data de criação, de modificação, de fechamento, tempo em que o chamado está aberto, número de alertas agregados, prioridade e analistas envolvidos;
 - ii. Classificação inicial da ameaça, incluindo categoria, origem (interna/externa), possibilidade de modificação manual da prioridade e justificativa, além de informações específicas para subsidiar o relatório

- de incidentes e possibilidade de inclusão de documentação adicional através da anexação de arquivos;
- iii. Possibilidade de manter o histórico de atividades realizadas pelos analistas, tais como criação de registros, atualização de campos, etc;
 - iv. Permitir agregar vários alertas em um único incidente. Esta agregação de alertas deverá permitir a visualização rápida de, no mínimo, os seguintes campos: horário do alerta, nome, prioridade e fonte (SIEM);
 - v. Definição das tarefas a serem executadas. A plataforma deverá conter uma biblioteca de procedimentos de resposta já existente;
 - vi. Permitir inserir comentários dos analistas no incidente, de tal forma a possibilitar o registro de todas as atividades de análise;
 - vii. Permitir inserir análise forense de host e rede como um complemento da análise do incidente;
 - viii. Inserir informações de impacto ao negócio incluindo: impacto geral ao negócio, tipo de perda de negócio, rating de perda pro negócio, unidades de negócio afetadas, além de permitir a inclusão de riscos identificados;
 - ix. Inserir análise de impacto relativo a Confidencialidade, incluindo informações existentes sobre Brecha de Segurança tais como data, status, dispositivos envolvidos e descrição;
 - x. Inserir análise de impacto relativo a Integridade, incluindo informações existentes sobre rating de comprometimento de integridade e tipo de integridade comprometida;
 - xi. Inserir análise de impacto relativo a Disponibilidade, incluindo informações existentes sobre rating de comprometimento de disponibilidade e tipo de disponibilidade comprometida;
 - xii. Permitir criar Ações de Remediação que incluam Contenção, Erradicação, Educação de usuários e melhorias no programa do SOC;\
 - xiii. Permitir registrar os resultados de um Incidente incluindo sua confirmação, categoria de ataque, identificação de técnicas utilizadas, detalhes sobre o alvo dos ataques e eficácia dos controles de detecção, prevenção e investigação;
- d) Permitir o recebimento de Alertas de Segurança com as seguintes características:
- i. Nome do alerta, fonte geradora, prioridade, data de criação, data original do alerta, categoria, ação, tipo, nível de severidade, descrição, serviço afetado, e detalhes do alerta;
 - ii. Dados de origem e destino, portas de origem e destino, domínios de origem e destino, endereço MAC de origem e destino, além de informações de contexto de negócios de cada dispositivo (de origem ou destino). As informações de contexto deverão incluir endereço IP, nome do dispositivo, tipo, unidade de negócios, site, índice de criticidade e conformidade, além do proprietário, tanto para os dispositivos de origem quanto dispositivos de destino. É necessário também incluir informações de localização do dispositivo, incluindo cidade, país e geolocalização tanto dos dispositivos de origem quanto dos dispositivos de destino dos alertas;
 - iii. Capacidade de incluir arquivos anexos, de acordo com a necessidade de aprofundamento de detalhes dos alertas;

- e) Permitir a criação de Investigações de Incidentes que não sejam necessariamente relacionados a Segurança da Informação, que permitam o atendimento às seguintes características:
- f) Data de criação, status, prioridade, dias em aberto, tipo de investigação (exemplo: hacking, má conduta, violação de ética, etc), identificação de confidencialidade, datas de início e término da investigação, título, sumário, analista atribuído, nome do solicitante, fonte, tipo de requisição, nível de urgência;
 - i. Definição do time de investigadores (proprietário, coordenador, gestor, funcionário de RH, responsável por Compliance, departamento jurídico. Inclusão de documentação através de arquivos anexos e eventuais conexões com Incidentes de Segurança já existentes;
 - ii. Possibilidade de inclusão de comentários de atividades por parte dos analistas, permitindo desta forma a identificação clara de todo o processo investigativo;
 - iii. Definição de procedimentos investigativos. A plataforma deverá conter uma biblioteca de procedimentos investigativos já existente;
 - iv. Inserir informações de impacto ao negócio incluindo: impacto geral ao negócio, tipo de perda de negócio, rating de perda pro negócio, unidades de negócio afetadas, além de permitir a inclusão de riscos identificados;
 - v. Inserir análise de impacto relativo a Confidencialidade, incluindo informações existentes sobre Brecha de Segurança tais como data, status, dispositivos envolvidos e descrição;
 - vi. Inserir análise de impacto relativo a Integridade, incluindo informações existentes sobre rating de comprometimento de integridade e tipo de integridade comprometida;
 - vii. Inserir análise de impacto relativo a Disponibilidade, incluindo informações existentes sobre rating de comprometimento de disponibilidade e tipo de disponibilidade comprometida;
 - viii. Permitir criar Ações de Remediação que incluam Contenção, Erradicação, Educação de usuários e melhorias no programa do SOC;
 - ix. Permitir registrar os resultados de um Incidente incluindo sua confirmação, categoria de ataque, identificação de técnicas utilizadas, detalhes sobre o alvo dos ataques e eficácia dos controles de detecção, prevenção e investigação;
- g) Possibilitar o registro de Análise Forense, tanto para rede quanto para host. Este registro deverá atender às seguintes características:
 - i. Analista, título, notas, data de criação e de atualização, resultado e conexão com Incidentes de Segurança;
 - ii. Detalhes da análise forense realizada em host com, no mínimo, as seguintes informações: dispositivo alvo (MAC, tipo, nome do dispositivo, sistema operacional, unidade de negócios, localidade, criticidade do dispositivo, proprietário, endereço IP). Inclusão de relatórios externos para servir como documentação de apoio, além da identificação de artefatos utilizados na análise. Deverá ser possível a inclusão dos arquivos suspeitos através de funcionalidade de inclusão de arquivos anexos;
 - iii. Detalhes da análise forense realizada na rede com, no mínimo, as seguintes informações: título, confirmação de intrusão, fonte, destino e identificação do tráfego de rede suspeito;

- h) Permitir a inclusão de novos procedimentos de Resposta a Incidentes com as seguintes informações: Nome do procedimento, fonte, versão, categoria de ameaça, conexão com Incidentes de Segurança, e tarefas detalhadas que incluem ordem da tarefa, nome, definição quanto a ser opcional ou requerida, status e observações.

2.5.2 PROCESSO DE RESPOSTA A INCIDENTE DE SEGURANÇA DA INFORMAÇÃO.

- 2.5.2.1 Um incidente de segurança é definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação do CONTRATANTE, levando a perda de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade. Logo o início do processo de resposta a incidente de segurança se dará, sempre que um evento adverso for submetido pelo SERVIÇOS DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS descrito no presente termo de referencia, porém não se limitando a este. Poderá o corpo técnico de segurança do CONTRATANTE a qualquer tempo, abrir um incidente de segurança.
- 2.5.2.2 Afim de balizar todo o processo de resposta a incidente de segurança do CONTRATANTE, e influenciado pelos principais frameworks de boas praticas de serviços de segurança da informação, foi arquitetado o processo que será descrito nos parágrafos que seguem, o qual obrigatoriamente a CONTRATADA deve seguir *ipsis litteris*.
- 2.5.2.3 O processo de resposta a incidente de segurança é iniciado, assim que o grupo de triagem de eventos realizar a abertura de incidente de segurança na ferramenta descrita no tópico SOBRE AS FERRAMENTAS A SEREM UTILIZADAS.
- 2.5.2.4 Após o incidente de segurança aberto, será de responsabilidade do grupo de resposta a incidente de segurança (CSIRT – Blue Team) da CONTRATADA, analisar os logs e artefatos enviados, afim de no primeiro instante identificar as fontes geradoras de tais logs.
- 2.5.2.5 Uma vez realizado as análises iniciais do incidente gerado, o grupo de resposta a incidente de segurança (CSIRT – Blue Team) da CONTRATADA, deverá trabalhar para identificar quais foram os principais vetores de ataque ao ambiente do CONTRATANTE.
- 2.5.2.6 Como próximo passo o grupo de resposta a incidente de segurança (CSIRT – Blue Team) da CONTRATADA, deverá comunicar ao time de segurança da informação do CONTRATANTE as informações iniciais sobre o incidente de segurança gerado, e quais serão as linhas de atuação para solução do incidente.
- 2.5.2.7 Juntamente com o CONTRATANTE o grupo de resposta a incidente de segurança (CSIRT – Blue Team) da CONTRATADA, deverá definir a severidade do incidente de segurança. A severidade do incidente de segurança da informação será definida através da combinação de urgência e impacto, onde impacto é definido como a medida de criticidade do negócio referente ao incidente, e urgência refere-se à velocidade necessária para resolver um incidente. Mais detalhes sobre definição da severidade se encontram no tópico ACORDO DE NÍVEIS DE SERVIÇO.

- 2.5.2.8 Após análises iniciais do incidente, caberá ao o grupo de resposta a incidente de segurança (CSIRT – Blue Team), realizar uma análise mais profunda do incidente baseando-se no comportamento do ataque e/ou artefato (malware).
- 2.5.2.9 Todo o processo de análise e resultados obtidos, devem ser documentados a todo tempo na ferramenta de gestão de incidente da segurança da informação, para que o CONTRATANTE acompanhe todos os passos para a solução do incidente.
- 2.5.2.10 Uma vez identificado comportamento e os principais vetores de ataque, o grupo de resposta a incidente de segurança (CSIRT – Blue Team) da CONTRATADA, deverá definir e executar uma estratégia para a mitigação e contenção do ataque em questão. Caso seja necessário qualquer tipo de alteração no parque computacional do CONTRATANTE, para contenção e mitigação do incidente, deverá antes ser autorizado tal alteração pelo corpo técnico de segurança do CONTRATANTE.
- 2.5.2.11 Mitigado o incidente de segurança, o próximo passo exigido é que a CONTRATADA através do grupo de resposta a incidente de segurança (CSIRT – Blue Team), inicie o processo de recolhimento de toda e quaisquer evidências, e identificação dos serviços afetados. Tais evidências serão utilizadas até a finalização do processo, para execução de análise forense do caso.
- 2.5.2.12 Inicia-se então o processo de restauração dos serviços e soluções afetadas. Todo este processo é de responsabilidade da CONTRATADA, sendo realizado pelo grupo de resposta a incidente de segurança (CSIRT – Blue Team) da CONTRATADA.
- 2.5.2.13 Deve-se reunir os dados coletados durante o processo de tratamento de incidente, para iniciar o processo de análise forense do mesmo, ainda pelo grupo de resposta a incidente de segurança (CSIRT – Blue Team). Tal análise deve ser realizada com o objetivo de identificar (pessoas, locais e/ou eventos), correlacionando todas as informações reunidas, e gerando como produto final um laudo sobre o incidente de segurança em questão.
- 2.5.2.14 Caso seja necessário a reconstrução do ataque, este deve ser realizado pela CONTRATADA em ambiente controlado, usando-se por exemplo de sandbox (mecanismo de segurança para separar programas em execução, geralmente utilizado em um esforço para mitigar falhas de sistema ou vulnerabilidades de segurança da informação). Tal ambiente deve ser de propriedade e controle da CONTRATADA.
- 2.5.2.15 O grupo de resposta a incidente de segurança (CSIRT – Blue Team) da CONTRATADA, deve documentar na ferramenta de incidente de segurança, as lições aprendidas do incidente de segurança em questão, formando durante todo o período de vigência do contrato uma grande base de conhecimento sobre ataques adversos.

2.5.3 GRUPO TÉCNICO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

- 2.5.3.1 Através do seus 2 (dois) CSOC do inglês Cyber Security Operations Center definidos no tópico CSOC - CYBER SECURITY OPERATIONS CENTER., a CONTRATADA deverá manter uma torre de operação denominada GRUPO DE RESPOSTA A INCIDENTE DE SEGURANÇA (CSIRT – Blue Team), com objetivo e foco de trabalhar no processo de monitoramento de ataques cibernéticos.
- 2.5.3.2 Este grupo deverá ser exclusivo para trabalhar no **Erro! Autoreferência de indicador não válida.**, não podem os profissionais pertencentes a este grupo serem compartilhados e/ou atuarem, com os demais serviços descritos no objeto do presente termo de referência.
- 2.5.3.3 Todos os profissionais que integram o GRUPO DE RESPOSTA A INCIDENTE DE SEGURANÇA (CSIRT – Blue Team), devem obrigatoriamente compor o quadro de colaboradores da CONTRATADA em regime de trabalho CLT (Consolidação das Leis do Trabalho), não havendo possibilidade a terceirização ou subcontratação de tal serviço.
- 2.5.3.4 Deverá ser de responsabilidade da CONTRATADA dimensionar o número de profissionais adequado para entrega de tal serviço, sem que haja impacto no acordo de nível de serviço estabelecido no tópico ACORDO DE NÍVEIS DE SERVIÇO do presente termo de referência.
- 2.5.3.5 Afim de garantir que os profissionais envolvidos têm conhecimento e habilidade, para executar o processo de resposta a incidente de segurança do CONTRATANTE, a CONTRATADA obrigatoriamente deverá compor o GRUPO DE RESPOSTA A INCIDENTE DE SEGURANÇA (CSIRT – Blue Team), com ao menos 1 (um) perfil de cada que segue descrito abaixo:

Perfis	Certificações	Descrição
Analista de Segurança I	CompTIA Security+	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.
Analista de Segurança II		Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de

	ComTIA Cybersecurity Analyst (CySA+)	certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação
Analista de Segurança III	Certified Ethical Hacker Linux LPIC 2 Linux LPIC 3	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 5 (cinco) anos em segurança da informação

TABELA 4 - CERTIFICAÇÕES [GRUPO DE RESPOSTA A INCIDENTE DE SEGURANÇA (CSIRT)]

- 2.5.3.6 Não existe restrição ou limite para acúmulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos no GRUPO DE RESPOSTA A INCIDENTE DE SEGURANÇA (CSIRT), porém conforme já fora mencionado no presente termo de referência, este(s) deve(m) compor único e exclusivamente o time denominado GRUPO DE RESPOSTA A INCIDENTE DE SEGURANÇA (CSIRT).
- 2.5.3.7 No momento da assinatura do contrato será exigido da CONTRATADA, as seguintes documentações do(s) profissionais que participarão do GRUPO DE RESPOSTA A INCIDENTE DE SEGURANÇA (CSIRT), os quais devem comprovar as exigências e obrigações descritas no presente termo de referência: carteira de trabalho devidamente assinada pela CONTRATADA, curriculum vitae para comprovação de habilidades, e as devidas certificações técnicas para comprovação do conhecimento.

2.5.4 ENTREGAS A SEREM REALIZADAS

- 2.5.4.1 Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, o CONTRATANTE definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue de forma on line e em tempo de execução, através do portal de segurança descrito através do anexo III do presente termo de referência, a saber:

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Quantitativo de incidentes abertos	Soma de incidentes abertos	Incidentes abertos	Incidentes	Número total de incidentes abertos
Quantitativo de incidentes que resultaram em comprometimento da segurança	Soma de incidentes abertos que resultaram em comprometimento da segurança	Incidentes com comprometimento	Incidentes com comprometimento	Número total de incidentes com comprometimento
Quantitativo de incidentes que tenham potencial de comprometer a segurança	Soma de incidentes que tenham potencial de comprometer a segurança	Incidentes com potencial	Incidentes com potencial	Número total de incidentes com potencial
Quantitativo de incidentes que não tenham potencial de comprometer a segurança	Soma de incidentes que não tenham potencial de comprometer a segurança	Incidentes sem potencial	Incidentes sem potencial	Número total de Incidentes sem potencial
TOP 10 – IP de destino de incidentes de segurança	Soma do número de incidentes por IP de destino	Incidentes abertos/tratados por IP de destino	IP de destino	TOP do número de incidentes por IP de destino
TOP 10 – Incidentes de segurança por origem	Soma do número de incidentes por origem	Incidentes abertos/tratados por origem	Origem	TOP do número de incidentes por origem interna ou externa
TOP 10 – Tipos de Incidentes	Soma do número de incidentes por tipo	Incidentes abertos/tratados por tipo	Tipo	TOP 10 por tipo de incidente

TABELA 10 - INDICADORES ESTRATÉGICOS DE RESPOSTA A INCIDENTES DE SEGURANÇA

- 2.5.4.2 Tais relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços prestados e com uma das seguintes certificações: CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager, CIA (Certified Intrusion Analyst), GSEC (GIAC Security Essentials), GCIH (GIAC Incident Handler) ou GMON (GIAC Continuous Monitoring), conforme condições expostas no tópico QUALIFICAÇÃO TÉCNICA DOS PROFISSIONAIS DA EMPRESA:. Nesse contexto, o profissional deve apresentá-lo de forma

presencial nas dependências do CONTRATANTE ou de forma virtual, por meio de solução de videoconferência.

3 DA MENSURAÇÃO

3.1. O pagamento será feito mensalmente, levando-se em consideração o Nível Mínimo de Serviço (NMS) acordado em contrato, para o período de faturamento avaliado. O valor a ser pago será o valor unitário do item correspondente, alinhado com NMS acordado em contrato.

3.1.1. Conforme ACORDO DE NÍVEIS DE SERVIÇO os SERVIÇOS GERENCIADOS DE SEGURANÇA, serão medidos a saber:

- a) **DISPONIBILIDADE MENSAL DOS GRUPOS DE TECNOLOGIAS:** Acompanha a execução do “SERVIÇOS GERENCIADOS DE SEGURANÇA” sobre os ativos de segurança descritos no tópico AMBIENTE TECNOLÓGICO DO CONTRATANTE (HARDWARE E SOFTWARE), sobre responsabilidade da CONTRATADA.
- b) **ENTREGA MENSAL DOS SERVIÇOS:** Acompanha a execução de todos os demais serviços que compõem o objeto SERVIÇOS GERENCIADOS DE SEGURANÇA, sobre os ativos de segurança descritos no tópico AMBIENTE TECNOLÓGICO DO CONTRATANTE (HARDWARE E SOFTWARE), sobre responsabilidade da CONTRATADA.

3.1.2. Logo de forma a viabilizar a análise da prestação dos serviços, a CONTRATADA deverá apresentar, através do seu portal de segurança descrito através do anexo III, informações acerca da aferição dos níveis de serviço contratados. Tais informações deverão estar agrupados conforme medição proposta acima, e obrigatoriamente deverão ter a disposição abaixo:

a) **DISPONIBILIDADE MENSAL DOS GRUPOS DE TECNOLOGIAS:**

GRUPO DE TECNOLOGIA	MDM	PD	FAIS
Proteção de Dados			
Inspeção e Conformidade do Fluxo de Rede			
VTAI (Valor R\$ total apurado)			

TABELA 5 - DASHBOARD DISPONIBILIDADE DOS GRUPOS DE TECNOLOGIAS

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR
Grupo de tecnologia	N/A	N/A	N/A
MDM - Meta de disponibilidade mensal do item	Conforme tópico - DISPONIBILIDADE MENSAL DOS GRUPOS DE TECNOLOGIAS	Período de apuração	Grupo de tecnologia

PD - Percentual de disponibilidade mensal.	Conforme tópico - DISPONIBILIDADE MENSAL DOS GRUPOS DE TECNOLOGIAS	Período de apuração	Grupo de tecnologia
FAIS - Fator de abatimento por indisponibilidade de serviço	Conforme tópico - DISPONIBILIDADE MENSAL DOS GRUPOS DE TECNOLOGIAS	Período de apuração	Grupo de tecnologia
VTAI (Valor R\$ total apurado)	Soma do total de FAIS, e subtrai do valor total previsto para o serviço gestão de disponibilidade.	Período de apuração	N/A

TABELA 6 - LEGENDA DISPONIBILIDADE DOS GRUPOS DE TECNOLOGIAS

b) ENTREGA MENSAL DOS SERVIÇOS:

TIPO DE PRIORIDADE	QUANTIDADE DE ATENDIMENTO REALIZADO NO PERÍODO	QUANTIDADE DE ATENDIMENTO DESACORDO COM O NMS	FATOR DE ABATIMENTO POR DESEMPENHO DE SERVIÇO (FADS)
P1			
P2			
P3			
P4			
P5			
P6			
P7			
P8			
VTAD (Valor R\$ total apurado)			

TABELA 7 - DASHBOARD DE ENTREGA DE SERVIÇOS

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR
Tipo de prioridade	N/A	N/A	N/A
Quantidade de atendimento realizado no período	Soma de todos os atendimentos realizados no período	Período de apuração	Prioridade
Quantidade de atendimento desacordo com	Soma de todos os atendimentos realizados no	Período de apuração	Prioridade

o NMS	período que não estão em conformidade com o NMS supracitado		
Fator de abatimento por desempenho de serviço (FADS)	Conforme item ENTREGA MENSAL DOS SERVIÇOS GERENCIADOS DE SEGURANÇA	Período de apuração	Prioridade
VTAD (Valor R\$ total apurado)	Soma do total de FADS, e subtrai do valor total previsto para o período	Período de apuração	N/A

TABELA 8 - LEGENDA DE ENTREGA DE SERVIÇOS

- 3.1.3. A reunião mensal deverá ocorrer até o 5o (quinto) dia útil após o termino do período de faturamento, que coincidirá com o mês legal, e a disponibilidade dos relatórios será condição necessária ao recebimento dos serviços pelo CONTRATANTE. O primeiro mês de faturamento será parcial, contado da data da emissão do termo de recebimento definitivo até o último dia do mês.
- 3.1.4. A respectiva nota fiscal/fatura, já deduzidos os fatores de abatimento calculados, deverá ser emitida somente após o recebimento definitivo dos serviços e após a homologação das informações apresentadas pela CONTRATADA ao CONTRATANTE.
- 3.1.5. Caso não haja concordância, por parte da CONTRATADA, em relação aos fatores de abatimento calculados, os mesmos serão convertidos em sanção, com aplicação de multa de mesmo valor, de forma a garantir o contraditório e a ampla defesa.
- 3.1.6. A qualquer tempo e a critério do CONTRATANTE, a bases dos sistemas utilizados para calculo das entregas e indicadores listados neste tópico, podem ser solicitadas para auditorias e aferições.
- 3.1.7. E, finalmente, o pagamento dos "SERVIÇOS GERENCIADOS DE SEGURANÇA" será feito após a ordem de serviço ser emitida e os serviços prestados de maneira satisfatória, conforme modelo de Termo de Recebimento de Serviços, respeitados os prazos definidos no item Serviços Técnicos Especializados. A nota fiscal/fatura relativa à prestação dos serviços, já considerado os fatores de abatimento (FADS e FAIS), deverá ser emitida somente após o recebimento dos serviços pelo CONTRATANTE.

4 DA ABRANGÊNCIA E ESCOPO DOS SERVIÇOS:

- 4.1 Considerar-se-á, para efeitos desta contratação, todos os recursos necessários para sua efetiva prestação dos serviços.

- 4.2 O dimensionamento da equipe para execução adequada do serviço contratado é de responsabilidade exclusiva do Fornecedor de Serviço, devendo ser suficiente para o cumprimento integral dos níveis de serviço exigidos neste Termo de Referência.
- 4.3 Dependendo da complexidade, criticidade e do prazo do projeto os serviços poderão ser realizados nas instalações da CONTRATADA ou do CONTRATANTE.
- 4.4 Atualmente o CONTRATANTE possui contrato de SERVIÇOS GERENCIADOS DE SEGURANÇA nas metodologias ITIL e NIST, assim a CONTRATADA deverá ser capaz de atender os projetos nestas duas metodologias.
- 4.5 Todos os custos com licenças de simuladores, dispositivos físicos, hardware, software ou demais equipamentos devem estar contabilizados no valor do serviço, não sendo permitido o pagamento de valores adicionais ou extra.

5 EXECUÇÃO DOS SERVIÇOS

- 5.1 A CONTRATADA deverá atender às seguintes condições gerais para início de prestação de cada um dos serviços, incluindo fase de concepção da solução, confecção de Projeto Executivo, planejamento de atividades de instalação, customização de ambiente e ativação de serviços, sem ônus adicionais ao CONTRATANTE:
 - a) Serão de responsabilidade da CONTRATADA as atividades de instalação, integração, configuração e testes de todos os produtos componentes de cada solução alocada, excluindo-se a Solução de Segurança do Sistema CONTRATANTE já ativa, em conformidade com o Projeto Executivo a ser elaborado e apresentado pela CONTRATADA para aprovação pelo CONTRATANTE;
 - b) A CONTRATADA deverá levantar informações acerca dos locais de instalação dos produtos durante a elaboração do Projeto Executivo, e, se pertinente, efetuar visita técnica para verificar eventuais requisitos físicos a serem providos para a correta instalação e prestação dos serviços;
 - c) As visitas técnicas poderão ser realizadas nos dias úteis, das 08:30h as 17:30h, mediante agendamento prévio;
 - d) Independentemente da alocação dos racks pela CONTRATADA, esta deverá efetuar a reorganização dos racks existentes, de forma a acomodar os seus equipamentos, quando necessário;
 - e) A elaboração do Projeto Executivo estará a cargo da CONTRATADA e deverá conter as fases do projeto, os cronogramas de execução e a descrição detalhada dos produtos e subprodutos a serem entregues em cada fase, respeitando o prazo máximo total de 60 (sessenta) dias para a entrega de todos os serviços previstos, a contar da assinatura do contrato;
 - f) Conter a descrição de topologia lógica e física da rede atual e topologia pretendida em cada etapa;
 - g) Efetuar o mapeamento de criticidade de todos os ativos envolvidos no projeto, inclusive os de propriedade do CONTRATANTE;
 - h) Projetar a engenharia de tráfego da Rede CONTRATANTE;
 - i) Planejar a migração das configurações do parque atualmente em funcionamento;
 - j) Para implantação dos serviços, indicar de forma detalhada as condições de rollback de cada mudança no ambiente do Sistema CONTRATANTE;
 - k) Estimar o consumo de unidades de rack em U's e de energia de cada ativo a ser instalado nas dependências do CONTRATANTE;

- 5.2 Os equipamentos, softwares e demais componentes necessários à correta prestação dos serviços deverão:
- a) Conter os recursos necessários e estarem configurados de modo a garantir total operabilidade no ambiente computacional do Sistema CONTRATANTE, e otimizados para usufruir das melhores condições em termos de desempenho e disponibilidade;
 - b) Conter a última versão de software e firmware homologado pelo fabricante;
 - c) Ter configuradas senhas de acesso para que a equipe de funcionários designados pelo CONTRATANTE efetue o acesso para a visualização das configurações e logs (acesso seguro e remoto);
 - d) Ter configurada senha com direitos totais de administração e configuração a ser utilizada pelo CONTRATANTE em caso de emergência;
 - e) Ser configurados para enviar logs para as soluções de concentração de logs disponibilizados no site do CONTRATANTE;
- 5.3 Todos os recursos para implantação dos serviços providos pela CONTRATADA serão por ela providenciados, sem ônus para o CONTRATANTE. Incluem-se, entre outros:
- a) Cabeamento de rede para interligação ao switch core da rede e demais ativos necessários ao funcionamento adequado da solução;
 - b) Cabeamento de energia elétrica para alimentação dos equipamentos e respectivos adaptadores;
 - c) Quaisquer materiais, cabos, parafusos, porcas, conectores elétricos, tomadas, adaptadores ou acessórios necessários ao cumprimento dos requisitos dos diversos serviços;
- 5.4 Para aprovação da instalação e configuração de qualquer item que enseje a emissão de termo de recebimento definitivo, a CONTRATADA deve elaborar relatório técnico com análise dos resultados e impactos decorrentes da atividade executada;
- 5.5 As atividades quando realizadas no ambiente de produção poderão ser agendadas para serem executadas após o expediente (horários noturnos, após as 20h, ou em finais de semana e feriados), conforme disponibilidade do CONTRATANTE;
- 5.6 A operação assistida deverá obedecer aos requisitos a seguir:
- a) Iniciará quando forem finalizados o planejamento, a customização de ambiente e a instalação dos ativos de rede, sendo o item de serviço submetido para recebimento definitivo.
 - b) A mudança para o ambiente de produção será concomitante a este momento, salvo se expressamente solicitado pelo CONTRATANTE que seja feita em data diferente; terá duração de 30 dias e será executada nas dependências do CONTRATANTE, em horário comercial (8:30h às 17:30h);
 - c) Caso seja necessária a consecução de atividades, pelo técnico responsável pela operação assistida, que possam afetar a disponibilidade de serviços de Rede do CONTRATANTE, estas devem ocorrer após as 20:00h;
- 5.7 Caso o CONTRATANTE encontre pendências impeditivas à emissão do termo de recebimento definitivo, a operação assistida deverá ser prorrogada até que sejam sanados os motivos geradores das pendências;

- 5.8 Caso a implantação de um serviço cause interferência no funcionamento de qualquer funcionalidade no Sistema CONTRATANTE, a CONTRATADA deverá alocar profissionais com qualificação suficiente para corrigir o problema ou retornar o ambiente à condição anterior à implantação.
- 5.9 A CONTRATADA deverá implementar e documentar para todos os componentes da solução as configurações de segurança necessárias, que visem à redução do risco de acesso indevido a cada servidor (hardening), como, por exemplo, remoção de serviços desnecessários do sistema operacional, configurações de kernel, configurações dos serviços ativos para suas permissões mínimas de funcionamento, remoção de usuários- padrão de sistemas e aplicativos, além de eventuais configurações para resistir a ataques de negação de serviço.
- 5.10 Para o planejamento e o acompanhamento da instalação dos equipamentos e softwares necessários à execução dos serviços, da entrega das etapas para recebimento definitivo, da confecção do Projeto Executivo, da confecção do as- built, e para demais atividades pertinentes até a emissão do termo de recebimento definitivo de todos os itens, a CONTRATADA deverá alocar GERENTES DE PROJETOS que possuam qualificação Project Management Professional (PMP) e/ou, Prince2 Practitioner Certificate in Project Management, e/ou Professional Scrum Master I.

6 SOLICITAÇÃO DOS SERVIÇOS TÉCNICOS

- 6.1 Conforme supracitado no presente termo de referência no tópico DA PROPOSTA DE PREÇO, os serviços que compõem objeto SERVIÇOS GERENCIADOS DE SEGURANÇA, foram agrupados, a saber:
- a) SERVIÇOS GERENCIADOS DE SEGURANÇA – DEMANDA INICIAL: Serviços os quais o CONTRATANTE, já possui necessidade imediata.
 - b) SERVIÇOS GERENCIADOS DE SEGURANÇA – DEMANDA FUTURA: Serviços os quais o CONTRATANTE, terá necessidade futura.
- 6.2 Os SERVIÇOS GERENCIADOS DE SEGURANÇA – DEMANDA INICIAL, serão solicitados e passarão a serem executados em totalidade, consequentemente faturados pela CONTRATADA em totalidade, a partir do termo de recebimento definitivo, emitido pós a habilitação do contrato, onde mais detalhes poderão ser apreciados no tópico EXECUÇÃO DOS SERVIÇOS.
- 6.3 Os SERVIÇOS GERENCIADOS DE SEGURANÇA – DEMANDA FUTURA serão solicitados por meio de Ordens de Serviços – OS, a serem emitidas pela Unidade de Tecnologia da Informação e Comunicação do CONTRATANTE, respeitando-se o que dispõe este instrumento.
- 6.4 As Ordens de Serviços deverão obrigatoriamente identificar:
- a) Número da Ordem de Serviço.
 - b) Data da Emissão;
 - c) Unidade Solicitante;
 - d) Nome do responsável solicitante que deverá acompanhar a execução e declarar, no encerramento, a qualidade dos serviços prestados;
 - e) Telefone e e-mail do solicitante;

- f) Objeto dos Serviços: Deverá ser descrito o escopo que o serviço pretende atender;
 - g) Descrição do processo de negócio, dos requisitos ou outros documentos complementares, onde serão especificadas as necessidades gerais a serem contempladas pelo projeto e que possam ser úteis para que a CONTRATADA realize a especificação dos serviços;
 - h) Quantidade total de esforço estimado para conclusão dos serviços;
 - i) Cronograma Físico-Financeiro: Planejamento da execução das atividades e os correspondentes desembolsos proporcionais, que deverão ocorrer em um determinado período;
 - j) Data máxima para conclusão: Determinar o prazo em que se pretende que o serviço esteja concluído;
 - k) Artefatos/produtos a serem produzidos: Definição do produto;
 - l) Descrição das tarefas: Descrever as principais tarefas a serem realizadas;
 - m) Dados da Autorização: Nome/cargo/telefone do autorizador dos serviços e data da autorização;
- 6.5 Eventuais erros ou disfunções encontradas serão reportados oficialmente para a CONTRATADA que deverá proceder as correções sem ônus para o CONTRATANTE.
- 6.6 Os produtos onde não forem detectadas não conformidades, receberão o termo de aceite, documento necessário ao processo de pagamento do serviço.
- 6.7 O termo de aceite não exclui a CONTRATADA de responsabilidade de erros não detectados e nem a exime da responsabilidade sobre a qualidade, garantia e manutenção corretiva dos serviços.
- 6.8 Os SERVIÇOS GERENCIADOS DE SEGURANÇA – DEMANDA FUTURA, poderão não somente atender ao CONTRATANTE, bem como também todas as suas filiais e/ou regionais.
- 6.9 Especificamente para o SERVIÇOS TÉCNICOS ESPECIALIZADOS previstos dentro do grupo de SERVIÇOS GERENCIADOS DE SEGURANÇA – DEMANDA FUTURA, só poderão ser utilizados no cenário onde o objeto da Ordem de Serviço, NÃO conflitar sobre nenhuma hipótese com o objeto já previsto no grupo de SERVIÇOS GERENCIADOS DE SEGURANÇA – DEMANDA INICIA.

7 ACORDO DE NÍVEIS DE SERVIÇO

- 7.1 A prestação dos serviços será baseada no modelo de remuneração em função dos resultados apresentados, em que os pagamentos serão feitos após mensuração e verificação de métricas quantitativas e qualitativas, contendo indicadores de desempenho e metas, com Nível Mínimo de Serviço (NMS) definido em contrato, de modo a resguardar a eficiência e a qualidade na prestação dos serviços.
- 7.2 Os níveis mínimos de serviço contratados serão registrados, monitorados e comparados às metas de desempenho e qualidade estabelecidas, em termos de prazo e efetividade, condição fundamental para efetuar os pagamentos previstos.
- 7.3 De modo a facilitar a compreensão dos Níveis Mínimos de Serviço (NMS) dos Serviços Gerenciados de Segurança, são apresentadas, a seguir, exigências mínimas em termos de níveis de serviço que devem ser atendidas pela CONTRATADA na execução do contrato, a saber:

7.4 DISPONIBILIDADE MENSAL DOS GRUPOS DE TECNOLOGIAS

7.4.1 Para os itens 1 a 5 dos Serviços Gerenciados de Segurança, a Meta de Disponibilidade Mensal (MDM) por grupo de tecnologia deve ser de, no mínimo:

item	Grupo de Tecnologia	MDM (%)	FPI
1	Proteção de Dados	99	1,75
2	Injeção e Conformidade de Fluxo de Redes	98	1,5

TABELA 9 - META DE DISPONIBILIDADE MENSAL

7.4.2 Os SERVIÇOS GERENCIADOS DE SEGURANÇA foi arquitetado para garantir e medir a disponibilidade do parque de segurança da informação descrito no tópico AMBIENTE TECNOLÓGICO DO CONTRATANTE (HARDWARE E SOFTWARE) do presente termo de referência, logo o mesmo deverá ser utilizado para apurar a meta de disponibilidade mensal (MDM).

7.4.3 Em cada período avaliado, o cálculo do Percentual de Disponibilidade Mensal (PDM) por item de serviço deve ser calculado com a seguinte fórmula:

$$PDM_k = \frac{[TM - TI_k]}{TM} * 100$$

PDM_k = Percentual de Disponibilidade Mensal do k-ésimo item de serviço;

k = k-ésimo item de serviço;

TM = Tempo total mensal de operação, em minutos, no mês de faturamento;

TI_k = Tempo total mensal de indisponibilidade do k-ésimo item de serviço, em minutos, no mês de faturamento.

7.4.4 Devem ser incluídos como Tempo de Indisponibilidade (TI_k):

- Tempo em que o respectivo serviço esteja indisponível ou com desempenho degradado;
- Tempo decorrente entre o início da indisponibilidade do serviço e a sua total recuperação;

7.4.5 Não devem ser incluídos como Tempo de Indisponibilidade (TI_k):

- Falta de energia no local de prestação dos serviços;
- Indisponibilidade da rede lógica do CONTRATANTE;
- Problemas derivados de ocorrências no ambiente do CONTRATANTE, onde comprovadamente a indisponibilidade não esteja sendo controlada pela CONTRATADA;
- Ações necessárias para resolução de problemas que tenham sido autorizadas pelo CONTRATANTE;
- Indisponibilidade gerada pela operadora de telecomunicação responsável pelos links e equipamentos da Rede CONTRATANTE;
- Indisponibilidade gerada pela necessidade de reparo ou troca dos equipamentos da solução de segurança da informação da rede CONTRATANTE, listadas do tópico AMBIENTE TECNOLÓGICO DO CONTRATANTE (HARDWARE E SOFTWARE) do presente termo de referência;

- g) Fatores externos a prestação de serviços, desde que justificado e acordado com o time de segurança do CONTRATANTE;
- h) Indisponibilidade do ambiente virtualizado do CONTRATANTE, infraestrutura computacional em que parte dos *softwares* que compõe a solução devem ser instalados;
- i) Manutenções programadas pelo CONTRATANTE;
- j) Manutenções programadas pela CONTRATADA, desde que previamente autorizadas pelo CONTRATANTE.

7.4.6 Tickets abertos cujo o prazo de resolução encerre somente no próximo período de faturamento somente terão calculados os fatores de abatimento a partir do período seguinte;

7.4.7 Os fatores de abatimento por indisponibilidade de serviços (FAIS) relativos ao percentual de disponibilidade mensal deverão, ainda, ser multiplicados por um fator de peso do item (FPI), segundo a TABELA 9 - META DE DISPONIBILIDADE MENSAL, por grupo de tecnologia.

7.4.8 O Percentual de Disponibilidade Mensal (PDM) é subsidiário para o cálculo do Fator de Abatimento por Indisponibilidade de Serviço (FAIS), desconto a ser aplicado no valor de prestação mensal de cada conjunto ou item de serviço;

7.4.9 Assim sendo, o Fator de Abatimento por Indisponibilidade de Serviço (FAIS) deve ser calculado de acordo com a seguinte fórmula:

$$FAIS = \sum_{k=1}^{10} VMI_k \times FPI_k \times \left\{ \frac{MDM_k - \text{MIN}(MDM_k, PD_k)}{100} \times MTI \right\}$$

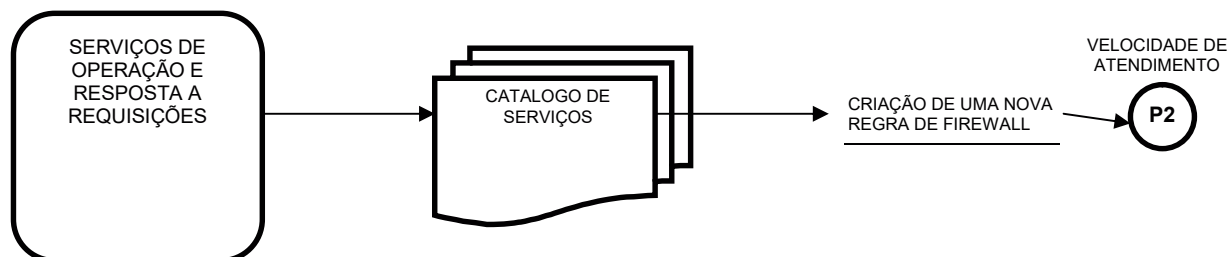
Variável	Descrição
k	Numero do grupo de tecnologia
FAIS	Fator de abatimento por indisponibilidade de serviço
VMI	Valor mensal do item de serviço de Gestão de Disponibilidade
MDM	Meta de disponibilidade mensal do item
PD	Percentual de disponibilidade mensal, calculada segundo formula supracitada.
MTI	Multiplicador por tempo de indisponibilidade, conforme definido a seguir: Valor = 1, se (MDM - PD) menor igual 1; Valor = 1, se (MDM - PD) maior que 1 e menor igual a 5; Valor = 1, se (MDM - PD) for maior que 5;
Min	Função que retorna o valor mínimo.

TABELA 10 - VARIÁVEIS DE CALCULO DE FATOR DE ABATIMENTO POR INDISPONIBILIDADE DE SERVIÇO (FAIS)

7.5 ENTREGA MENSAL DOS SERVIÇOS GERENCIADOS DE SEGURANÇA

7.5.1 Além da meta de disponibilidade mensal do parque de segurança da informação do CONTRATANTE, a qual avalia especificamente o SERVIÇOS GERENCIADOS DE SEGURANÇA, deverão também ser apurados os níveis de serviço para os demais serviços que somados compõem o objeto Serviços Gerenciados de Segurança.

- 7.5.2 Todos os serviços que compõem o objeto contratado, possui catalogo de serviço descrito no anexo XX do presente termo de referência. Cada item (serviços) que compõem o catalogo de serviço, estar relacionado com os tipos de velocidade de atendimento, descritos na tabela XXX do presente termo de referência, conforme exemplo ilustrado na figura abaixo:



Tipos	Nível mínimo de serviço (NMS)	IndMeta	Fator de peso da Atividade (FAT)
P1	2 Horas	2 Horas	1
P2	4 Horas	4 Horas	1
P3	8 Horas	8 Horas	0,5
P4	16 Horas	16 Horas	0,5
P5	32 Horas	32 Horas	0,5
P6	64 Horas	64 Horas	0,25
P7	128 Horas	128 Horas	0,25
P8	256 Horas	256 Horas	0,25

TABELA 11 - NIVEIS DE PRIORIDADES DE ATENDIMENTO

- 7.5.3 Em um atendimento onde seja necessária uma janela para execução dos serviços solicitados, os tempos entre a necessidade do atendimento e janela de execução deverão ser excluídos.
- 7.5.4 Os fatores de abatimento por desempenho de serviço (FADS) serão calculados com base na comparação dos resultados alcançados na execução das atividades com os níveis de serviços definidos na TABELA 11 - NIVEIS DE PRIORIDADES DE ATENDIMENTO.
- 7.5.5 O FADS será calculado como somatório das ocorrências realizadas para cada uma das atividades definidas, conforme fórmula a seguir:

$$FADS = \sum_{i=1}^8 \sum_{j=1}^n VMC \times \left[\frac{\text{Max} (INDATINGi, j, INDMETAi) - INDMETAi}{10 \times INDMETAi} \right] \times FPAi$$

Variável	Descrição
i	Tipo de prioridade.
j	Contador de ocorrências do tipo de prioridade que não atenderam o NMS definido.

n	Quantidade de ocorrências do tipo de prioridade que não atenderam o NMS definido.
FADS	Fator de abatimento por desempenho de Serviço
VMC	Valor mensal do contrato.
INDMETA	Índice de meta (NMS), em minutos/horas/dias, definido para a atividade.
INDATING	Índice atingido, em minutos/horas/dias, pela atividade que ultrapassou o (NMS).
FPA	Fator de peso da atividade.
Max	Função que retorna o valor máximo.

TABELA 12 - VARIÁVEIS DE CÁLCULO DE FATORES DE ABATIMENTO POR DESEMPENHO DE SERVIÇO (FADS)

8 PAPÉIS E RESPONSABILIDADE

8.1.1 Deverá ser empregada na prestação de serviço deste contrato, os seguintes papéis e responsabilidades dos profissionais:

- a) Patrocinador do Projeto (CONTRATANTE): é o gerente da Unidade de Tecnologia da Informação, responsável por representar os interesses do CONTRATANTE no contexto da presente contratação, pela aprovação da necessidade, dos objetivos e, por fim, pela negociação das ações necessárias para a melhoria da Governança de TI;
- b) Gestor do Contrato (CONTRATANTE): é o funcionário formalmente designado pelo CONTRATANTE, responsável pelo monitoramento da prestação do serviço ao longo do período de vigência do contrato, pelo controle da evolução dos gastos com o contrato, pela proposição de aditamentos ao contrato, pela participação no planejamento da contratação, pela verificação dos resultados pretendidos e por garantir que a metodologia adequada seja empregada;
- c) Gerente da Demanda (CONTRATANTE): é o funcionário que aprova a execução do serviço, executa os processos de gerenciamento, monitoramento e controla o andamento de projetos. Auxilia as equipes terceirizadas a remover eventuais obstáculos que possam impedir a equipe de produzir, garantindo o foco no resultado. Zela pela colaboração entre os diferentes papéis e pela melhoria dos processos, atuando sempre como um facilitador. É quem fornece insumos ao Gestor do Contrato quanto à regular execução do serviço prestado, em relação aos níveis de serviço esperados e às demais disposições contratuais;
- d) Gestor de Negócio (CONTRATANTE): é o funcionário da unidade de negócio do CONTRATANTE que representa e/ou assessora o demandante do produto. Responsável pela liderança do produto que será desenvolvido, priorizando as funcionalidades que agregam maior valor para o negócio. Tem também o papel de elucidar questões relacionadas ao negócio junto ao Fornecedor de Serviço como também homologar os produtos entregues.
- e) Preposto (CONTRATADA): é o profissional indicado pelo Fornecedor de Serviço para representá-la administrativa e tecnicamente. É o responsável pela coordenação operacional das atividades previstas nos projetos, de forma a solucionar qualquer dúvida, conflito ou desvio técnico que possa comprometer a execução das OS.

Deverá ter bons conhecimentos em gestão de projetos para garantir o controle sobre os sinais vitais de cada projeto. Também é responsável pela interlocução com o Gestor do Contrato do CONTRATANTE;

- 8.1.2 Os requisitos da qualificação técnica destes profissionais estão especificados no tópico **QUALIFICAÇÃO TÉCNICA DOS PROFISSIONAIS DA EMPRESA:**, supracitada no presente termo de referência.

9 DA PROPOSTA DE PREÇO

- 9.1. A Proposta de preço deverá seguir os padrões estabelecidos no item **MODELO DE PROPOSTA** do presente termo de referência.

10 QUALIFICAÇÃO TÉCNICA DOS PROFISSIONAIS DA EMPRESA:

As qualificações técnicas exigidas para os profissionais que executarão o serviço contratado deverão ser comprovadas por meio de diplomas, certificados, registros em carteira de trabalho, contratos de trabalho assinados.

- 10.1. As qualificações técnicas exigidas para o perfil de **GERENTE DE PROJETO** da **CONTRATADA**:

Certificações	Descrição
Ao menos uma das certificações de segurança da informação: • Project Management Professional (PMP); • Prince2 Practitioner Certificate in Project Management; • Professional Scrum Master I;	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em gerencia de projetos, com experiência mínima de 5 (cinco) anos.

TABELA 13 - QUALIFICAÇÕES GERENTE DE PROJETO

- 10.2. As qualificações técnicas exigidas para o perfil de **PREPOSTO** da **CONTRATADA**:

Certificações	Descrição
Ao menos uma das certificações de segurança da informação: • CISSP (Certified Information Systems Security Professional); • CISM (Certified Information Security)	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC);

• Manager; • CIA (Certified Intrusion Analyst), • GSEC (GIAC Security Essentials); • GCIH (GIAC Incident Handler) • GMON (GIAC Continuous Monitoring);	Conhecimento avançado em segurança da informação, com experiência mínima de 5 (cinco) anos em coordenação e gestão de contratos de serviços continuados.

TABELA 14 - QUALIFICAÇÕES PREPOSTO

- 10.3. As qualificações técnicas exigidas para o perfil de analista(s) que participará do supracitado GRUPO DE ATAQUE CIBERNÉTICO CONTROLADO (Red Team) da CONTRATADA:

Certificações	Descrição
• CompTIA Security+ • Linux LPIC 1 • Linux LPIC 2 • Linux LPIC 3 • Certified Ethical Hacker	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.

TABELA 15 - QUALIFICAÇÕES GRUPO DE ATAQUE CIBERNÉTICO CONTROLADO (RED TEAM)

- 10.4. As qualificações técnicas exigidas para o perfil de analista(s) que participará do supracitado GRUPO DE MONITORAMENTO DE ATAQUES da CONTRATADA:

Perfis	Certificações	Descrição

Analista de Segurança I	CompTIA Security+	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.
Analista de Segurança II	ComTIA Cybersecurity Analyst (CySA+)	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação
Analista de Segurança III	- Certified Ethical Hacker - Linux LPIC 2 - Linux LPIC 3	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 5 (cinco) anos em segurança da informação

TABELA 16 - QUALIFICAÇÕES GRUPO DE MONITORAMENTO DE ATAQUES

- 10.5. As qualificações técnicas exigidas para o perfil de analista(s) que participará do supracitado GRUPO DE RESPOSTA A INCIDENTE DE SEGURANÇA (CSIRT – Blue Team), da CONTRATADA:

Perfis	Certificações	Descrição
Analista de Segurança I	CompTIA Security+	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.
Analista de Segurança II	ComTIA Cybersecurity Analyst (CySA+)	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação
Analista de Segurança III	- Certified Ethical Hacker - Linux LPIC 2 - Linux LPIC 3	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC);

		Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 5 (cinco) anos em segurança da informação

TABELA 17 - QUALIFICAÇÕES GRUPO DE RESPOSTA A INCIDENTE DE SEGURANÇA (CSIRT – BLUE TEAM)

10.6. As qualificações técnicas exigidas para o perfil de analista(s) que participará do supracitado GRUPO SOLUCIONADOR, da CONTRATADA:

Perfis	Certificações	Descrição
Analista de Segurança I	CompTIA Security+	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.
Analista de Segurança de Perímetro II	CCSA – Check Point Certified Security Administrator CompTIA Advanced Security Practitioner certificate	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação
Analista de Segurança de		Diploma, devidamente registrado, de curso de nível superior de graduação na área de

Endpoint	CompTIA Security+ Linux LPIC 2 Linux LPIC 3	Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação

TABELA 18 - QUALIFICAÇÕES GRUPO SOLUCIONADOR

11 QUALIFICAÇÃO TÉCNICA DA EMPRESA:

- 11.1. As qualificações técnicas da empresa, estão descritas em todo o decorrer do texto do presente termo de referência, o tópico em questão, resume tais qualificações, todavia a caso algumas das qualificações não esteja listadas no presente tópico, porém no em algum paragrafo do termo de referencia, NÃO exime da obrigatoriedade da CONTRATADA em apresentar tais qualificações, inclusive no caso de não atendimento a qualquer um dos itens deste termo de referencia, ensejará na desclassificação da empresa licitante participante.
- 11.2. Atestados de Capacidade Técnica (ACT) em nome da CONTRATADA emitido(s) por pessoa(s) jurídica(s) de direito público ou privado, onde comprove ter prestado ou estar prestando:
- SERVIÇOS GERENCIADOS DE SEGURANÇA em regime de 24 (vinte quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, em ambiente compatível ao CONTRATANTE;
 - Serviços de Firewall, por meio do fornecimento e instalação de equipamentos ou prestação de serviços de suporte ou assistência técnica, em redes com, no mínimo, 1.000 (um mil) estações de trabalho, incluindo desktops e notebooks;
 - Serviço de Prevenção de Intrusão (IPS), por meio do fornecimento e instalação de equipamentos ou prestação de serviços de suporte ou assistência técnica, em redes com, no mínimo, 1.000 (Um mil) estações de trabalho, incluindo desktops e notebooks;
 - Serviços de Filtragem WEB, ou Gateway Antispam ou Firewall de Aplicação, por meio do fornecimento e instalação de equipamentos ou prestação de serviços de suporte ou assistência técnica, em redes com, no mínimo, 1.000 (Um mil) estações de trabalho, incluindo desktops e notebooks;

- e) Serviços de Administração e Monitoramento de Segurança, por meio do fornecimento e instalação de equipamentos ou prestação de serviços de administração e monitoramento de segurança em redes com, no mínimo, 1.000 (Um mil) ativos de TI;
 - f) Serviço de Gestão de Vulnerabilidades, por meio do fornecimento e instalação de equipamentos ou prestação de serviços de suporte ou assistência técnica, os quais devem monitorar e tratar, no mínimo, 1.000 (Um mil) ativos de TI;
 - g) Os serviços supracitados podem estar distribuídos em diversos atestados de capacidade técnica, não se exigindo que todos sejam prestados a uma única pessoa jurídica de direito público ou privado;
- 11.3. Não será admitida a soma de atestados de forma a atingir os quantitativos exigidos em cada um dos serviços elencados nos itens “a”, “b”, “c”, “d”, “e” e “f”, do presente tópico.
- 11.4. Os atestados de capacidade técnica deverão comprovar que os serviços foram prestados por um período mínimo de 12 (doze) meses.
- 11.5. Estas exigências se fazem necessárias no intuito de verificar a experiência e a habilidade técnica da licitante na execução do objeto desta licitação;
- 11.6. A CONTRATADA deverá apresentar ainda, declaração, datada e assinada por seu representante legal, de que, caso se sagre vencedora do certame, no momento da assinatura do contrato, disporá, no mínimo, de profissionais com as qualificações técnicas listadas no tópico QUALIFICAÇÃO TÉCNICA DOS PROFISSIONAIS DA EMPRESA:, listadas no presente termo de referência.
- 11.7. A CONTRATADA deverá apresentar ainda, declaração, datada e assinada por seu representante legal, de que, caso se sagre vencedora do certame, no momento da assinatura do contrato, disporá, no mínimo, as certificações referente ao CSOC - CYBER SECURITY OPERATIONS CENTER. em seu NOME, já supracitada no referente termo, a saber:

item	Certificações
1	ABNT NBR ISO/IEC 27001
2	ABNT NBR ISO/IEC 20001
3	ABNT NBR ISO/IEC 9001

TABELA 19 - CERTIFICAÇÕES DO CSOC DA CONTRATADA

12 MODELO DE PROPOSTA

- 12.1. A proposta de preços deverá conter separadamente o valor de cada serviço (item do objeto) observando-se as unidades de medida referente a cada serviço, conforme planilhas abaixo:

SERVIÇOS GERENCIADOS DE SEGURANÇA – DEMANDA INICIAL			
#	ITEM	QUANTIDADE	VALOR UNITÁRIO
1			
2	Serviços de monitoramento de ataques cibernéticos	30	R\$ 0,00
3	Serviços de resposta a incidentes de segurança	30	R\$ 0,00
4	Serviços de operação e resposta a requisições	30	R\$ 0,00
5		30	R\$ 0,00
6			
7			
8			
VALOR TOTAL			

- 12.2. Todos os participantes deverão apresentar a planilha de composição de custos acima anexa à proposta comercial, seguindo o padrão do anexo V.
- 12.3. Devem ser informadas as marcas, modelos e quantidades de todos os equipamentos, produtos, peças ou softwares necessários à correta prestação dos serviços, assim como a descrição de como será feito o atendimento aos requisitos do Termo de Referência.
- 12.4. O preço total de cada item será igual ao valor unitário multiplicado pelo limite máximo do item especificado.
- 12.5. O preço global da proposta será a soma de todos os preços totais. Importante ressaltar que o CONTRATANTE está contratando um único serviço denominado SERVIÇOS GERENCIADOS DE SEGURANÇA, logo para efeito de concorrência será considerado o valor global da proposta.
- 12.6. Nos preços apresentados deverão estar incluídas todas as despesas com materiais, mão-de-obra, links, deslocamentos, manutenção corretiva, hospedagens, ferramentas, equipamentos, seguros, taxas, tributos, incidências fiscais e contribuições de qualquer natureza ou espécie, encargos sociais, salários, custos diretos e indiretos e quaisquer outros encargos, necessárias à perfeita execução do objeto da licitação.
- 12.7. Os preços apresentados deverão constar todos os custos diretos e indiretos, tais como despesas com materiais, links, mão-de-obra, ferramentas, equipamentos, seguros, taxas, tributos, incidências fiscais, contribuições de qualquer natureza ou espécie, salários, encargos sociais, salários, deslocamentos, hospedagens, e quaisquer outros encargos necessários à perfeita execução do objeto da licitação.

13 PRAZOS DE EXECUÇÃO E DE ACEITE E NATUREZA DOS SERVIÇOS

- 13.1. Os serviços serão contratados inicialmente por 36 meses, podendo ser prorrogado, até o limite de 60 meses de contrato. O período de prestação, a partir da emissão do termo de recebimento definitivo, será o estabelecido na tabela abaixo, observadas as

etapas previstas no item EXECUÇÃO DOS SERVIÇOS do presente termo de referência.

#	ITEM	QUANTIDADE	MESES
1		30	30
2	Serviços de monitoramento de ataques cibernéticos	30	30
3	Serviços de resposta a incidentes de segurança	30	30
4			
5			
6			
7			
8			

14 INSPEÇÕES E DILIGÊNCIAS

- 14.1. O CONTRATANTE reserva-se o direito de efetuar inspeções e diligências para sanar quaisquer dúvidas existentes, podendo efetuar a contratação;
- 14.2. O CONTRATANTE realizará diligência no CSOC - CYBER SECURITY OPERATIONS CENTER. da licitante participante no momento da análise da qualificação, in loco, afim de validar e aferir se TODOS os itens solicitados neste Termo de Referência serão atendidos;
- 14.3. O NÃO ATENDIMENTO A QUALQUER UM DOS ITENS DESTE TERMO DE REFERÊNCIA ENSEJARÁ NA DESCLASSIFICAÇÃO DA EMPRESA LICITANTE PARTICIPANTE.

15 AMBIENTE TECNOLÓGICO DO CONTRATANTE (HARDWARE E SOFTWARE)

15.1 PROTEÇÃO DE DADOS E DATACENTER

- a) O ambiente possui 300 usuários;
- b) O ambiente possui 13 servidores Linux;
- c) O ambiente possui 54 servidores Windows;
- d) O ambiente possui 1 link de internet com largura de banda de 200 Gbps;

FABRICANTE	DESCRIÇÃO	QUANTIDADE
Trend Micro	DeepSecutiry	40
Symantec	SEP	330
Symantec	SMG	1
HP	DL 380 Gen	13
Netapp	2552	1
AZURE	BACKUP	1
VERITAS	BACKUP	1
HP	1/8 G2 Autoloader	1

15.2 INSPEÇÃO E CONFORMIDADE DE FLUXO DE REDE

FABRICANTE	DESCRIÇÃO	QUANTIDADE
SonicWall	NSa 3650	2
EXTREME	X460G2- 24T10G4	5
AVAYA	G450	4

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 17.^a REGIÃO

TERMO DE CONTRATO TRT 17.^a REGIÃO N.º 07/2022

Contrato de prestação de serviço técnico especializado de monitoramento de ameaças cibernéticas que entre si celebram a União, por intermédio do Tribunal Regional do Trabalho da 17.^a Região, e a empresa Intelliway Tecnologia LTDA.

Aos primeiro (01.º) dias do mês de abril de 2022, na sede do Tribunal Regional do Trabalho da 17.^a Região, situada na Avenida Nossa Senhora dos Navegantes, n.º 1245, Enseada do Suá, Vitória/ES, CEP: 29050-335, de um lado **a UNIÃO**, por intermédio do **Tribunal Regional do Trabalho da 17.^a Região**, inscrito no CNPJ/MF sob o n.º 02.488.507/0001-61, neste ato representado por seu presidente, o Exmo. Desembargador Marcello Maciel Mancilha, ou por seu substituto legal, doravante também designado CONTRATANTE ou TRT e, de outro lado, a empresa **Intelliway Tecnologia LTDA.**, estabelecida na Rua Roberto da Silva, n.º 20, Edifício Premium Office, Sala 310, Anexo Torre B, Mata da Praia, Vitória/ES, CEP: 29066-091, inscrita no CNPJ/MF sob o n.º 21.337.573/0001-85, neste ato representada por Carlos Eduardo Brandão, portador da Cédula de Identidade n.º 920.116 – SSP/ES, inscrito no CPF sob o n.º 017.133.287-39, daqui por diante denominada simplesmente CONTRATADA, têm entre si justo e avençado e celebram por força do presente instrumento, autorizado pelo despacho do Exma. Sra. Desembargadora-Presidente do TRT, exarado nos autos do **PAe n.º 0000292-72.2022.5.17.0500**, **contrato emergencial** para prestação de serviço técnico especializado de monitoramento de ameaças cibernéticas, em conformidade com o disposto na Lei n.º 14.133/21 e suas alterações, mediante as seguintes cláusulas e condições:

DO OBJETO

CLÁUSULA PRIMEIRA – O presente contrato tem como objeto a prestação de serviço técnico especializado de monitoramento do ambiente para prevenção de ameaças cibernéticas e resposta a incidentes de segurança da informação, conforme especificações constantes deste contrato e do Anexo I.

DA VIGÊNCIA DO CONTRATO

CLÁUSULA SEGUNDA – O presente contrato terá vigência de **12 (doze) meses**, contados de 01.º de abril de 2022.

Parágrafo Primeiro - Este contrato **não** poderá ser prorrogado, por se tratar de contratação emergencial.

Parágrafo Segundo - Os prazos terão início e vencimento em dia de expediente, excluído o primeiro e incluído o último, e o contrato terá validade e eficácia legal após a publicação do seu extrato no Diário Oficial da União.

DO PRAZO DE EXECUÇÃO

CLÁUSULA TERCEIRA – Os serviços objeto deste contrato serão prestados pelo período de **10 (dez) meses e 20 (vinte) dias**.

DO PREÇO

CLÁUSULA QUARTA – O contratante pagará à contratada, pela prestação do serviço objeto desta contratação, o valor total de **R\$2.628.312,10** (dois milhões seiscentos e vinte e oito mil trezentos e doze reais e dez centavos), conforme quadro demonstrativo abaixo:

Item	Descrição	Quant.	Valor Unitário	Valor total
1	Serviços Gerenciados de Monitoramento, Detecção e Notificação de Ataques Cibernéticos	10,66 meses	R\$101.825,00	R\$1.085.454,50
2	Serviços Gerenciados de Red Team (Testes de Invasão Periódicos)	3 execuções	R\$58.400,00	R\$175.200,00
3	Serviço de Password & Credential Assessment (avaliação do banco de dados de senhas)	10 execuções	R\$11.000,00	R\$110.000,00
4	Serviços Gerenciados de Gestão de Vulnerabilidades, Riscos e Conformidade	10,66 meses	R\$21.110,00	R\$225.032,60
5	Serviços de Resposta, Investigação, Mitigação e Análise Forense de Incidentes de Segurança	3.755 horas	R\$275,00	R\$1.032.625,00
Total Geral				R\$2.628.312,10

DO FATURAMENTO

CLÁUSULA QUINTA – Os serviços ora contratados serão faturados **mensalmente**, em moeda corrente nacional, após a prestação dos serviços, devendo o faturamento incluir os valores mensais relativos aos itens 1 e 4, e o quantitativo dos itens 2, 3 e 5 demandados no período.

Parágrafo Primeiro – A contratada deverá enviar, juntamente com a fatura, para ateste da fiscalização do TRT, os seguintes documentos, com identificação das horas demandadas em horário comercial e das horas executadas em horário não-comercial:

I - Relatório contendo os resultados dos serviços de Teste de Invasão e Password & Credential Assessment executados no período (Itens 2 e 3); e

II - Relatório contendo os serviços executados no período relativos à resposta, investigação, mitigação e análise forense de incidentes de segurança, bem como correção de vulnerabilidades identificadas e atuação na restauração e melhoria do ambiente tecnológico do Tribunal (Item 5).

Parágrafo Segundo - As Faturas deverão ser enviadas, **preferencialmente**, para os endereços eletrônicos segec@trtes.jus.br e setic@trtes.jus.br, ou entregues na Secretaria de Tecnologia da Informação e Comunicações do Tribunal Regional do Trabalho da 17.^a Região, situada na Avenida Nossa Senhora dos Navegantes, n.º 1245, 4.º andar, Enseada do Suá, Vitória/ES, CEP: 29050-335.

Parágrafo Terceiro - Os dados para emissão da Nota Fiscal são os seguintes:

- Razão Social: TRIBUNAL REGIONAL DO TRABALHO DA 17.^a REGIÃO

- Endereço: Avenida Nossa Senhora dos Navegantes, n.º 1245, Enseada do Suá, Vitória/ES, CEP: 29050-335
- CNPJ: 02.488.507/0001-61
- Telefone: (27) 3185-2069 e 3321-2571

DO RECEBIMENTO

CLÁUSULA SEXTA – Os serviços ora contratados serão recebidos pela Comissão de Recebimento e Fiscalização das seguintes formas:

I – Durante a execução contratual - Preliminarmente, mediante emissão de atestado de regularidade de prestação de serviços e cumprimento das demais obrigações contratuais (aceite), em até 5 (cinco) dias úteis após efetuada a entrega do documento fiscal.

II - Ao término deste contrato:

- a) **Provisoriamente**, após o transcurso do prazo total da prestação dos serviços objeto desta contratação, para efeito de posterior verificação da conformidade integral do objeto com as especificações técnicas presentes neste termo e no Projeto Básico.
- b) **Definitivamente**, após a devida comprovação da conformidade do objeto com as especificações constantes neste termo e no Projeto Básico, em até 10 (dez) dias úteis após o recebimento provisório.

DO PAGAMENTO

CLÁUSULA SÉTIMA – Os pagamentos serão efetuados em moeda corrente nacional, mediante crédito em conta bancária indicada pela CONTRATADA **até o 10.º (décimo) dia útil** após ter sido atestada a regularidade de prestação do serviço, podendo ser retidos pelo CONTRATANTE, de forma cautelar, os valores referentes a eventuais multas que se julguem aplicáveis. Transcorrido o prazo recursal sem que tenha havido recurso, ou após negado seu provimento, o valor retido será recolhido à União. Existindo provimento, será efetuado pagamento à contratada.

Parágrafo Primeiro – O vencimento de validade de qualquer certidão apresentada para fins de habilitação não impossibilitará o pagamento à contratada.

Parágrafo Segundo – Para que o pagamento seja efetuado é indispensável que a CONTRATADA tenha informado o seu domicílio bancário (nome e código do banco, código da agência e número da conta corrente).

Parágrafo Terceiro – Considerar-se-á, para todos os fins, como data de pagamento, o dia de emissão da Ordem Bancária pelo CONTRATANTE.

Parágrafo Quarto – A apresentação de faturas com incorreções implicará a sua devolução à CONTRATADA para regularização, passando o prazo de pagamento a ser contado a partir da data de sua reapresentação, se corrigidas as irregularidades.

Parágrafo Quinto - Os pagamentos a serem efetuados à CONTRATADA, pela prestação dos serviços objeto da contratação, obedecerão às disposições da Lei 9.430/96 e demais normas complementares.

DA DOTAÇÃO ORÇAMENTÁRIA

CLÁUSULA OITAVA – As despesas decorrentes da execução deste contrato, no exercício de 2022, correrão à conta dos recursos orçamentários da contratante, Programa de Trabalho 02.122.0033.4256.0032 – 168188, Elemento de despesa: 339040, ou, havendo alteração da dotação orçamentária no decorrer do exercício, daquela que vier a substituí-la.

Parágrafo Único – No exercício seguinte, as despesas correrão à conta da dotação orçamentária prevista para atender às despesas da mesma natureza e, para efeitos do disposto no artigo 92, inciso VIII, da Lei 14.133/2021, as informações relativas a todas as notas de empenho emitidas pelo TRT da 17.^a Região, que serão consideradas anexos a este contrato, estarão (encontram-se) disponíveis no Portal do Órgão (<http://www.trtes.jus.br/principal/transparencia/orcamento-e-financas/notas-de-empenho>), sendo atualizadas mensalmente.

DO REAJUSTAMENTO DOS PREÇOS

CLÁUSULA NONA – Os preços contratados são irredutíveis durante todo o período de vigência contratual.

DAS OBRIGAÇÕES DA CONTRATADA

CLÁUSULA DEZ – São obrigações da contratada, além das demais estabelecidas neste instrumento e nas normas regulamentadoras do objeto contratado:

- I** - Planejar, desenvolver, implantar, executar e manter os serviços objeto do contrato de forma satisfatória;
- II** - Encaminhar à comissão de fiscalização todas as faturas dos serviços prestados;
- III** - Assumir a responsabilidade pelos encargos fiscais e comerciais resultantes da contratação;
- IV** - Reportar ao contratante imediatamente qualquer anormalidade, erro ou irregularidades que possa comprometer a execução dos serviços e o bom andamento das atividades do Tribunal;
- V** - Acompanhar diariamente a qualidade dos serviços prestados com vistas a efetuar eventuais ajustes e correções de rumo;
- VI** - Guardar sigilo sobre dados e informações obtidos em razão da execução dos serviços contratados ou da relação contratual mantida com o contratante;
- VII** - Obedecer a todas as normas e procedimentos de segurança implementados no ambiente de TIC do contratante;
- VIII** - Responder por quaisquer danos causados diretamente a bens de propriedade do contratante, quando tenham sido causados por seus profissionais durante a execução dos serviços;
- IX** - Manter durante toda a vigência contratual todas as condições de habilitação e qualificação exigidas, sob pena das sanções previstas neste termo, devendo informar ao CONTRATANTE, imediata e formalmente, caso ocorra, a impossibilidade de manutenção dessas condições, justificando a ocorrência;
- X** - Atualizar documentação referente à habilitação em até 15 (quinze) dias, contados da data do recebimento da notificação;
- XI** – **Aceitar**, nas mesmas condições contratuais, as **supressões** que se fizerem necessárias no objeto contratual, **superiores a 25%** (vinte e cinco por cento) do valor contratado, mantidas as mesmas condições estipuladas para o objeto.
- XII** - Assinar o “Termo de Confidencialidade”, quando da assinatura do instrumento contratual, constante do Anexo II;

XIII - informar (e manter atualizado) o endereço eletrônico (e-mail) correto para o qual serão encaminhadas notificações ao longo da vigência desta contratação (inclusive quanto a possíveis multas). Será considerada notificada a partir do dia útil seguinte ao envio do e-mail. É dever da contratada monitorar a conta de correio eletrônico fornecido;

XIV - cumprir as exigências de reserva de cargos prevista em lei, bem como em outras normas específicas, para pessoa com deficiência, para reabilitado da Previdência Social e para aprendiz.

DAS OBRIGAÇÕES DO CONTRATANTE

CLÁUSULA ONZE – O CONTRATANTE obriga-se a:

I - Adotar todas as providências necessárias que viabilizem a execução do objeto do contrato;

II - Comunicar à Contratada, de imediato e por escrito, qualquer irregularidade constatada no cumprimento do objeto deste contrato, determinando, de imediato, a adoção de medidas necessárias à solução dos problemas;

III - Acompanhar e fiscalizar a execução do objeto contratual;

IV - Verificar e atestar as faturas da contratada, homologando os serviços prestados;

V - Efetuar os pagamentos devidos pela execução dos serviços, no prazo estabelecido.

DO ACOMPANHAMENTO E DA FISCALIZAÇÃO

CLÁUSULA DOZE – O acompanhamento e a fiscalização deste contrato serão exercidos por comissão designada pelo Secretário de Tecnologia da Informação e Comunicações do TRT, composta por, no mínimo, 3 (três) integrantes.

Parágrafo Único - Competirá à Comissão o gerenciamento do contrato, exigindo o cumprimento das formalidades e obrigações avençadas, bem como efetuar os esclarecimentos das dúvidas porventura existentes e encaminhar à Administração os casos de descumprimento contratual que impliquem na aplicação das penalidades previstas nas Sanções Administrativas

DAS SANÇÕES ADMINISTRATIVAS

CLÁUSULA TREZE - Com fundamento nos arts. 155 a 162 da Lei n.º 14.133/2021, a tabela a seguir consigna as condutas reprováveis dos contratados e as correspondentes sanções aplicáveis:

Infração	Sanção
a) Dar causa à inexecução parcial do contrato.	Advertência , quando não se justificar penalidade mais grave, e multa de 2% , calculada sobre o valor do contrato.
b) Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;	Na hipótese de não justificar penalidade mais grave: Impedimento de licitar e contratar pelo período de 3 (três) anos, além de multa de 10% , calculada sobre o valor do contrato.
* Dar causa à inexecução total do contrato;	Quando justificada penalidade mais grave: Declaração de inidoneidade para licitar ou contratar pelo

* Deixar de entregar documentação exigida; * Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado; * Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta; * Ensejar o retardamento da execução ou da entrega do objeto sem motivo justificado	período de 5 (cinco) anos, além de multa de 20%, calculada sobre o valor do contrato.
c) Apresentar declaração ou documentação falsa exigida ou prestar declaração falsa durante a execução do contrato; * Praticar ato fraudulento na execução do contrato; * Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza; * Praticar atos ilícitos com vistas a frustrar os objetivos da licitação; * Praticar ato lesivo previsto no art. 5.º da Lei n.º 12.846, de 1.º de agosto de 2013.	Declaração de inidoneidade para licitar ou contratar pelo período de 6 (seis) anos, além de multa de 30%, calculado sobre o valor do contrato.

Parágrafo Primeiro - Poderá o contratante optar por aplicar à Contratada as seguintes penalidades:

I – ADVERTÊNCIA – Nos casos em que a(s) falta(s) cometida(s) não acarretem atraso em conclusão de serviço ou execução de atividade do órgão ou em obrigatoriedade de execução de contratação emergencial. Sendo aplicada:

a) No primeiro caso de não manutenção das condições de habilitação, desde que haja seu restabelecimento no prazo máximo de 30 (trinta) dias após a Administração notificar a contratada para atualizar seus documentos;

b) Sempre que forem observadas irregularidades de pequena monta, para as quais a Contratada tenha concorrido. Nesse caso será aplicada quando ocorrer:

b.1) o descumprimento, não reincidente, das obrigações contratuais que não acarretem prejuízos financeiros para o Contratante;

b.2) a execução insatisfatória ou pequenos transtornos ao desenvolvimento dos serviços, desde que sua gravidade não recomende a aplicação de multa, impedimento de licitar ou contratar ou declaração de inidoneidade.

II - MULTAS ADMINISTRATIVAS - Será aplicada a penalidade de Multa Administrativa à contratada nas seguintes situações:

- a) Acúmulo de Advertências: O acúmulo de 5 (cinco) advertências durante a vigência do contrato, ensejará em **multa** administrativa no valor de **10%** (dez por cento) do valor mensal do contrato;
- b) Não manutenção das condições de habilitação por prazo superior a 30 (trinta) dias: **multa de 10%**, calculada sobre o valor total da proposta, se esta situação for constatada no momento da assinatura do contrato, ou de 3% sobre o valor contratado, se esta situação for constatada após a assinatura do contrato;
 - b.1) Reincidência na não manutenção das condições de habilitação, ainda que por prazo inferior a 30 (trinta) dias, ou em falta punível com advertência: **multa de 10%**, calculada sobre o valor total da proposta, se esta situação for constatada no momento da assinatura do contrato, ou de 6% sobre o valor contratado, se esta situação for constatada após a assinatura do contrato.
- c) Atraso injustificado na execução do contrato: **multa de 5%**, calculada sobre o valor contratado.

Parágrafo Segundo - Nenhuma multa moratória, ou somatório delas, poderá exceder a 10% (dez por cento) do valor total deste contrato, inclusive as reincidências de multas de mesma natureza.

Parágrafo Terceiro – A contratada será formalmente notificada pelo TRT, das sanções a ela aplicadas.

Parágrafo Quarto - Em caso de aplicação da sanção de multa sem que a contratada apresente recurso no prazo legal ou, se apresentado, não tiver obtido provimento, o valor correspondente à penalidade aplicada será deduzido dos pagamentos eventualmente devidos pelo contratante.

Parágrafo Quinto - No caso de insuficiência ou inexistência de crédito em favor da contratada, o recolhimento da multa aplicada deverá ser por ela efetivado no prazo de até 10 (dez) dias, contados da data da notificação, mediante GRU (Guia de Recolhimento da União) a ser emitida e encaminhada pela Divisão de Orçamento e Finanças (DOF) do TRT.

Parágrafo Sexto - Decorrido o prazo previsto no parágrafo anterior, sem que a contratada tenha efetuado o depósito devido, o valor da multa poderá ser inscrito em Dívida Ativa da União e encaminhado para cobrança judicial.

Parágrafo Sétimo - As penalidades descritas nesta cláusula, com exceção feita à Declaração de Inidoneidade e ao Impedimento de Licitar e Contratar, poderão ser aplicadas pelo Diretor-Geral do TRT.

Parágrafo Oitavo - A decisão de aplicação da sanção de Impedimento de Licitar e Contratar é de competência exclusiva da Presidência do TRT e a *Declaração de Inidoneidade é de competência do Tribunal Pleno*, superior instância administrativa do TRT.

DA EXTINÇÃO

CLÁUSULA CATORZE – São motivos para a extinção do presente contrato, assegurados o contraditório e a ampla defesa:

- a) Os relacionados no Art. 137, incisos I a V, VIII, IX e parágrafo 2.º da Lei 14.133/2021;
- b) Quando as condutas descritas no ar. 23 da Lei 12.527/11 tiverem repercussão que macule a imagem do TRT perante a sociedade.

Parágrafo Primeiro – A extinção deste contrato atenderá o disposto no Art. 138 da Lei 14.133/2021, podendo acarretar as consequências previstas no Art. 139 da mesma lei.

Parágrafo Segundo - A extinção deste contrato poderá ser determinada por ato unilateral e escrito da Administração, exceto no caso de descumprimento decorrente de sua própria conduta, conforme inciso I do art. 138 da Lei 14.133/2021.

DOS RECURSOS ADMINISTRATIVOS

CLÁUSULA QUINZE- A aplicação de qualquer penalidade obedecerá sempre aos princípios da legalidade, razoabilidade, proporcionalidade, motivação e publicidade, dentre outros, garantido o direito do contraditório e da ampla defesa.

Parágrafo Primeiro - Os prazos e formalidades para a defesa prévia, recurso, representação ou pedido de reconsideração, obedecerão àqueles indicados na Lei n.º 14.133/2021, em especial os arts. 157, 158 e 165 a 168.

Parágrafo Segundo - O recurso interposto deverá ser protocolizado no Setor de Protocolo, Expediente, Correspondência 2.ª instância (SEPEX 2), localizado na Avenida Nossa Senhora dos Navegantes, n.º 1245, Enseada do Suá, Vitória/ES, CEP: 29050-335, de segunda a sexta-feira, das 12 às 19 horas.

DA PROTEÇÃO DE DADOS

CLÁUSULA DEZESSEIS - O Contratante e a Contratada se comprometem a proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, relativos ao tratamento de dados pessoais, inclusive nos meios digitais, garantindo que:

I - o tratamento de dados pessoais dar-se-á de acordo com as bases legais previstas nas hipóteses dos arts. 7.º e/ou 11 da Lei 13.709/2018 (LGPD); e

II - o tratamento será limitado às atividades necessárias ao atingimento das finalidades de execução do contrato e do serviço contratado, utilizando-os, quando seja o caso, em cumprimento de obrigação legal ou regulatória, no exercício regular de direito, por determinação judicial ou por determinação da ANPD.

Parágrafo Primeiro - A Contratada cooperará com o Contratante no cumprimento das obrigações referentes ao exercício dos direitos dos Titulares previstos na LGPD e nas Leis e Regulamentos de Proteção de Dados em vigor e, também, no atendimento de requisições e determinações do Poder Judiciário, Ministério Público e Órgãos de controle administrativo.

Parágrafo Segundo - O Contratante e a Contratada se comprometem, ainda, à eliminação dos dados pessoais coletados em razão desta contratação com o encerramento do ajuste ou, se for o caso, após o transcurso do prazo legal de guarda da informação.

Parágrafo Terceiro - A Contratada deve garantir, além da disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem.

DA FUNDAMENTAÇÃO LEGAL, REGIME DE EXECUÇÃO e DA VINCULAÇÃO

CLÁUSULA DEZESSETE – O presente contrato é regido pela Lei n.º 14.133/2021 e alterações, além das demais disposições legais aplicáveis, tratando-se de hipótese de contratação emergencial, nos termos do inciso VIII do art. 75 da mesma Lei.

Parágrafo Primeiro – Os serviços objeto desta contratação serão prestados na forma de execução indireta e no regime de empreitada por preço global.

Parágrafo Segundo – Para todos os efeitos, fazem parte integrante deste contrato, independentemente de transcrição, os documentos a seguir relacionados:

- a) Projeto Básico elaborado pela Secretaria de Tecnologia da Informação e Comunicações (Setic) do TRT;
- b) A proposta apresentada pela CONTRATADA, datada de 22 de março de 2022, juntada ao doc. 08 dos autos do PAe n.º 0000292-72.2022.5.17.0500.

DO FORO

CLÁUSULA DEZOITO – As questões decorrentes da execução deste contrato que não possam ser dirimidas administrativamente serão processadas e julgadas na Justiça Federal, no Foro da Cidade de Vitória/ES, Seção Judiciária do Estado do Espírito Santo, com exclusão de qualquer outro, por mais privilegiado que seja.

E para firmeza e como prova de assim haver entre si ajustado e contratado, é lavrado o presente contrato, que, após lido e achado conforme, é assinado pelas partes contratantes, em 2 (duas) vias de igual teor e de mesmos efeitos legais.

MARCELLO MACIEL Assinado de forma digital
por MARCELLO MACIEL
MANCILHA:308170 **MANCILHA:308170391**
391 **Dados: 2022.04.01**
15:45:46 -03'00'

Representante legal do TRT 17.^a Região / Contratante

CARLOS EDUARDO Digitally signed by CARLOS
EDUARDO
BRANDAO:017133 **BRANDAO:01713328739**
28739 **Date: 2022.03.31 14:51:50**
-03'00'

CARLOS EDUARDO BRANDÃO
Intelliway Tecnologia LTDA. / Contratada

TERMO DE CONTRATO TRT 17.^a REGIÃO N.º 07/2022

ANEXO I

ESPECIFICAÇÃO DO OBJETO

1- Prestação de serviços para monitoramento 24 por 7, detecção e notificação a ameaças e ataques cibernéticos:

- 1.1** - A contratada deve monitorar todas as estações, ativos de rede, ativos de segurança e nuvem do contratante;
- 1.2** - A solução de monitoramento deve ser capaz de correlacionar eventos de diversas fontes para detecção eficiente de ataques cibernéticos;
- 1.3** - A solução de monitoramento deve detectar comportamentos anormais em ativos e tráfego de rede;
- 1.4** - A solução de monitoramento deve prover dashboard de monitoramento e alertas;
- 1.5** - Os serviços podem ser prestados de forma remota;
- 1.6** - A solução de monitoramento deve prover uma franquia mínima de 24 horas de serviço especializado para imediata atuação reação à incidentes ou vulnerabilidades no ambiente monitorado.

2 - Serviço especializado de testes de penetração (hacker ético) em sistemas e infraestrutura da contratante:

- 2.1** - Testes de Invasão de Rede Externa (via internet), a ser executado sob demanda;
- 2.2** - Teste de Invasão de Rede Interna, a ser executado sob de manda;
- 2.3** - Testes de simulação de Email-Phishing, a ser executado sob demanda.

3- Serviço de Password & Credential Assessment (avaliação de credenciais em serviços de diretório e banco de dados):

- 3.1** - Avaliar o nível de dificuldade de quebra de senhas, ou possíveis vazamentos de credenciais, a ser executado sob demanda;
- 3.2** - O serviço deve ser executado sem que senhas sejam fornecidas à contratada.

4- Serviços de Gestão de Vulnerabilidades, Riscos e Conformidade na infraestrutura:

- 4.1** - Serviço de análise de vulnerabilidades para até 200 servidores, ativos de rede, ativos de segurança e ativos em nuvem;
- 4.2** - Varredura contínua de vulnerabilidades, incluindo servidores, ativos críticos e perímetro Internet;
- 4.3** - Dashboard de riscos e conformidade;
- 4.4** - Dashboard de projetos de ações de remediação e metas.

5 - Prestação de serviço técnico especializado, em regime de banco de horas, com profissionais capacitados para atuar na resposta, investigação, mitigação e análise forense de incidentes de segurança, bem como correção de vulnerabilidades identificadas e atuação na restauração e melhoria do ambiente tecnológico do Tribunal:

5.1 - Recomendação de medidas para mitigação dos ataques e ameaças detectadas (adequação de regras de firewall, proteção de endpoint, atualização de sistema operacional, dentre outros);

5.2 - Apoio na implementação de ações de remediação e/ou mitigação de vulnerabilidades de segurança da informação;

5.3 - Assessoria para restauração do ambiente ao seu estado normal de operação;

5.4 - Definir, propor e executar uma estratégia para a mitigação e contenção do ataque;

5.5 - Investigar e identificar no ambiente alvo ameaças persistentes ou vulnerabilidades passíveis de exploração, propondo soluções para a sua mitigação e, quando possível, realizar o tratamento das ameaças identificadas;

5.6 - Os serviços deverão ser executados sob demanda da Contratante;

5.6.1 - Os serviços poderão ser prestados presencialmente ou remotamente, a critério da Contratante.

5.7 - A Contratada deverá fornecer relatório das horas e atividades executadas no mês para ateste e pagamento;

5.8 - Caso a Contratante demande execução de atividades fora do horário comercial, estas atividades consumirão o banco de horas com 50% de acréscimo, ou seja, 1h30m para cada hora trabalhada.

5.8.1 - Será considerado horário-comercial aquele compreendido entre 8 e 20h de dias úteis.

TERMO DE CONTRATO TRT 17.^a REGIÃO N.º 07/2022

ANEXO II - TERMO DE CONFIDENCIALIDADE

ACORDO DE CONFIDENCIALIDADE DE INFORMAÇÃO

A empresa **Intelliwey Tecnologia LTDA.**, inscrita no CNPJ/MF n.º 21.337.573/0001-85, com endereço na Rua Roberto da Silva, n.º 20, Edifício Premium Office, Sala 310, Anexo Torre B, Mata da Praia, Vitória/ES, CEP: 29066-091, doravante denominada CONTRATADA, neste ato representada por seu sócio, Sr. Carlos Eduardo Brandão, brasileiro, inscrito no CPF sob o n.º 017.133.287-39, residente e domiciliado na cidade de Vitória/ES, firma o presente ACORDO DE CONFIDENCIALIDADE DE INFORMAÇÃO, decorrente da realização do Termo de Contrato TRT 17.^a Região n.º 07/2022, que entra em vigor na data de sua assinatura, sendo regido mediante as cláusulas e condições seguintes:

1. DA INFORMAÇÃO CONFIDENCIAL

Para fins do presente Acordo, são consideradas INFORMAÇÕES SIGILOSAS, os documentos e informações transmitidos pela CONTRATANTE e recebidos pela CONTRATADA através de seus diretores, sócios, administradores, empregados, prestadores de serviço, prepostos ou quaisquer representantes. Tais documentos e informações não se limitam, mas poderão constar de dados digitais, desenhos, relatórios, estudos, materiais, produtos, tecnologia, programas de computador, especificações, manuais, planos de negócio, informações financeiras, e outras informações submetidas oralmente, por escrito ou qualquer outro tipo de mídia. Adicionalmente, a expressão INFORMAÇÕES SIGILOSAS inclui toda informação que a CONTRATADA possa obter através da simples visita às instalações da CONTRATANTE.

2. DOS LIMITES DA CONFIDENCIALIDADE DAS INFORMAÇÕES - Para fins do presente Acordo, não serão consideradas INFORMAÇÕES SIGILOSAS as que:

- 2.1 São ou tornaram-se públicas sem ter havido a violação deste Acordo pela CONTRATADA;
- 2.2 Eram conhecidas pela CONTRATADA, comprovadas por registros escritos em posse da mesma, antes do recebimento delas pela CONTRATANTE;
- 2.3 Foram desenvolvidas pela CONTRATADA sem o uso de quaisquer INFORMAÇÕES SIGILOSAS;
- 2.4 Venham a ser reveladas pela CONTRATADA quando obrigada por qualquer entidade governamental jurisdicionalmente competente;

2.4.1 Tão logo inquirida a revelar as informações, a CONTRATADA deverá informar imediatamente, por escrito, à CONTRATANTE, para que este requeira medida cautelar ou outro recurso legal apropriado;

2.4.2 A CONTRATADA deverá revelar tão somente as informações que forem legalmente exigidas;

3. DAS OBRIGAÇÕES DA CONTRATADA - Consiste nas obrigações da CONTRATADA:

3.1 Garantir que as Informações Confidenciais serão utilizadas apenas para os propósitos do contrato n.º 07/2022, e que serão divulgadas apenas para seus diretores, sócios, administradores, empregados, prestadores de serviço, prepostos ou quaisquer representantes, respeitando o princípio do privilégio mínimo;

3.2 Não divulgar, publicar, ou de qualquer forma revelar qualquer INFORMAÇÃO SIGILOSA recebida através da CONTRATANTE para qualquer pessoa física ou jurídica, de direito público ou privado, sem prévia autorização escrita da CONTRATANTE;

3.3 Garantir que qualquer INFORMAÇÃO SIGILOSA fornecida por meio tangível não deve ser duplicada pela CONTRATADA exceto para os propósitos descritos neste acordo;

3.4 A pedido da CONTRATANTE, retornar a ele todas as INFORMAÇÕES SIGILOSAS recebidas de forma escrita ou tangível, incluindo cópias, reproduções ou outra mídia contendo tais informações, dentro de um período máximo de 10 (dez) dias após o pedido;

3.4.1 Como opção para CONTRATADA, em comum acordo com a CONTRATANTE, quaisquer documentos ou outras mídias possuídas pela CONTRATADA contendo INFORMAÇÕES SIGILOSAS podem ser destruídas por ela;

3.4.1.1 A destruição de documentos em papel deverá seguir recomendação da norma DIN 32757-1: 4, ou seja, destruição do papel em partículas de, no mínimo, 2 x 15mm;

3.4.1.2 A destruição de documentos em formato digital deverá seguir a norma DoD 5220.22-M (ECE) ou o método descrito por Peter Guttmann no artigo “Secure Deletion of Data From Magnetic and Solid-State Memory” ou através da utilização de desmagnetizadores (degausser);

3.4.1.3 A destruição das INFORMAÇÕES SIGILOSAS que não estiverem nos formatos descritos nos itens 3.4.1.1 e 3.4.1.2 deverá ser previamente acordada entre a CONTRATANTE e a CONTRATADA;

3.4.1.4 A CONTRATADA deverá fornecer à CONTRATANTE certificado com respeito à destruição, confirmando quais as informações que foram destruídas e os métodos utilizados, dentro de um prazo máximo de 10 (dez) dias;

3.5 A CONTRATADA deverá dar ciência deste acordo a todos seus sócios, empregados, prestadores de serviço, prepostos ou quaisquer representantes que participarão da execução dos serviços objetos do contrato e, será responsável solidariamente por eventuais descumprimentos das cláusulas aqui descritas.

4. DA PROPRIEDADE DAS INFORMAÇÕES SIGILOSAS

4.1 A CONTRATADA concorda que todas as INFORMAÇÕES SIGILOSAS permanecem como propriedade da CONTRATANTE e que esta pode utilizá-las para qualquer propósito sem nenhuma obrigação com ela;

4.2 A CONTRATADA concorda ter ciência de que este acordo ou qualquer INFORMAÇÃO SIGILOSA entregue pela CONTRATANTE a ela, não poderá ser interpretado como concessão a qualquer direito ou licença relativa à propriedade intelectual (marcas, patentes, copyrights e segredos profissionais) à CONTRATADA;

4.3 A CONTRATADA concorda que todos os resultados dos trabalhos prestados por ela à CONTRATANTE, inclusive os decorrentes de especificações técnicas, desenhos, criações ou aspectos particulares dos serviços prestados, são reconhecidos, irrestritamente, neste ato, como de exclusiva propriedade do CONTRATANTE, não podendo a CONTRATADA reivindicar qualquer direito inerente à propriedade intelectual;

5. DOS PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO DA CONTRATANTE

5.1 A CONTRATADA declara que recebeu cópia e está ciente da Política de Segurança da Informação da CONTRATANTE;

5.2 A CONTRATADA declara que seguirá todas as políticas, normas e procedimentos de segurança da informação definidos e/ou seguidos pela CONTRATANTE;

6. DO PRAZO DE VALIDADE DO ACORDO

As obrigações tratadas neste acordo subsistirão permanentemente, mesmo após a conclusão dos serviços ou até que a CONTRATANTE comunique expressa e inequivocadamente, por escrito, à CONTRATADA, que as informações já não são mais sigilosas.

7. DAS PENALIDADES

Qualquer divulgação de dados, materiais, desenhos ou informações, obtidos em razão dos serviços por CONTRATADA, ou prepostos e seus funcionários, sem a respectiva autorização prévia, expressa e escrita da CONTRATANTE, implicará na obrigatoriedade de CONTRATADA ressarcir as perdas e danos experimentados pela CONTRATANTE, sem prejuízo das penalidades civis e criminais previstas em lei.

Vitória, 31 de março de 2022.

CARLOS EDUARDO
BRANDAO:0171332
8739

Digitally signed by CARLOS
EDUARDO
BRANDAO:01713328739
Date: 2022.03.31 14:52:11 -03'00'

CARLOS EDUARDO BRANDÃO
Intelliway Tecnologia LTDA. / Contratada

Contrato nº TRT 17ª Região 07/2022

Última atualização 04/04/2022

Local: Vitória/ES **Órgão:** TRIBUNAL SUPERIOR DO TRABALHO **Unidade executora:** 080019 - TRIBUNAL REGIONAL DO TRABALHO DA 17ª. REGIAO **Tipo:** Contrato (termo inicial)

Receita ou Despesa: Despesa

Data de divulgação no PNCP: 04/04/2022 **Data de assinatura:** 01/04/2022 **Vigência:** de 01/04/2022 a 01/04/2023

Id contrato PNCP: 00509968000148-2-000023/2022 **Fonte:** Compras.gov.br **Id contratação PNCP:** [00509968000148-1-000039/2022](#)

Objeto:

Prestação de serviço técnico especializado de monitoramento do ambiente para prevenção de ameaças cibernéticas e resposta a incidentes de segurança da informação.

Informação complementar:

Conforme especificações constantes deste contrato e do Anexo I.

VALOR CONTRATADO

R\$ 2.628.312,10

FORNECEDOR:

Nome/Razão social: INTELLIWAY TECNOLOGIA LTDA **CNPJ/CPF:** 21.337.573/0001-85 **Tipo:** Pessoa jurídica

Arquivos

Histórico

Nome	Data	Tipo	Baixar
20220/ContratoIntelliway.pdf	04/04/2022	Contrato	

Exibir: 1-1 de 1 itens

Página

< >

< Voltar



Criado pela Lei nº 14.133/21, o Portal Nacional de Contratações Públicas (PNCP) é o site eletrônico oficial destinado à divulgação centralizada e obrigatória dos atos exigidos em sede de licitações e contratos administrativos abarcados pelo novo diploma.

É gerido pelo Comitê Gestor da Rede Nacional de Contratações Públicas, um colegiado deliberativo com suas atribuições estabelecidas no Decreto nº 10.764, de 9 de agosto de 2021.

O desenvolvimento dessa versão do Portal é um esforço conjunto de construção de uma concepção direta legal, homologado pelos indicados a compor o aludido comitê.

A adequação, fidedignidade e correção das informações e dos arquivos relativos às contratações disponibilizadas no PNCP por força da Lei nº 14.133/2021 são de estrita responsabilidade dos órgãos e entidades contratantes.

✉ <https://portal.deservicos.economia.gov.br>

☎ 0800.978.9001

AGRADECIMENTO AOS PARCEIROS





TRIBUNAL REGIONAL FEDERAL DA 3ª REGIÃO
Av. Paulista, 1842 - Bairro Bela Vista - CEP 01310-936 - São Paulo - SP - www.trf3.jus.br

CONTRATO Nº 04.018.10.2022

TERMO DE CONTRATO DE PRESTAÇÃO DE SERVIÇO Nº 04.018.10.2022 QUE FAZEM ENTRE SI A UNIÃO, POR INTERMÉDIO DO TRIBUNAL REGIONAL FEDERAL DA 3ª REGIÃO E A EMPRESA S3CURITY TECNOLOGIA SERVIÇOS DE INFORMÁTICA LTDA.

PRESTAÇÃO DE SERVIÇOS DE MONITORAMENTO DE AMBIENTE TECNOLÓGICO, PREVENÇÃO DE AMEAÇAS CIBERNÉTICAS E RESPOSTA À INCIDENTES DE SEGURANÇA DA INFORMAÇÃO ATRAVÉS DA IMPLANTAÇÃO DE NOC (NETWORK OPERATIONS CENTER) E SOC (SECURITY OPERATIONS CENTER)

A **UNIÃO FEDERAL**, por intermédio do **TRIBUNAL REGIONAL FEDERAL DA 3ª REGIÃO**, com sede na Avenida Paulista nº 1.842, Torre Sul, Bela Vista, São Paulo – SP, inscrito no CNPJ sob o nº 59.949.362/0001-76, neste ato representado pela sua Presidente, Desembargadora Federal **MARISA FERREIRA DOS SANTOS**, eleita para o cargo, biênio 2022-2024, conforme Ata da 153ª Sessão Plenária Ordinária Administrativa híbrida, realizada ao primeiro dia do mês de dezembro do ano de dois mil e vinte e um, às quinze horas e trinta e cinco minutos, e Termo de Posse lavrado aos dois dias do mês de março de dois mil e vinte e dois, no uso das atribuições que lhe são conferidas pelo Regimento Interno do Tribunal Regional Federal da 3ª Região, doravante denominado **CONTRATANTE**, e a empresa **S3CURITY TECNOLOGIA SERVIÇOS DE INFORMÁTICA LTDA**, inscrita no CNPJ sob o nº 13.738.040/0001-87, estabelecida na Rua da Conceição nº 188, sala 2801A, Centro, Niterói – RJ, neste ato representada pelo Sr. **ELESSANDRO DA SILVA MOREIRA**, Diretor Executivo, portador da cédula de identidade RG nº 09.913.407-4 DETRAN/RJ, inscrito no Cadastro de Pessoas Físicas sob o nº 070.291.317-03, doravante designada **CONTRATADA**, tendo em vista o que consta no Processo nº 0048355-09.2022.4.03.8000 e em observância às disposições da Lei nº 8.666, de 21 de junho de 1993, da Lei nº 10.520, de 17 de julho de 2002, do Decreto nº 10.024, de 20 de setembro de 2019, do Decreto nº 7.746, de 05 de junho de 2012, da Lei Complementar nº 123, de 14 de dezembro de 2006, do Decreto nº 8.538, de 06 de outubro de 2015, da Lei nº 8.078, de 11 de setembro de 1990 – Código de Defesa do Consumidor, do Decreto nº 7.892, de 23 de janeiro de 2013, e da Instrução Normativa SEGES/MP nº 5, de 26 de maio de 2017 resolvem celebrar o presente Termo de Contrato, decorrente do Pregão Eletrônico nº 044/2022-RP, por Sistema de Registro de Preços, mediante as cláusulas e condições a seguir enunciadas.

1. CLÁUSULA PRIMEIRA – OBJETO

1.1. O objeto do presente instrumento é contratação de empresa especializada na prestação de serviços de monitoramento de ambiente tecnológico, prevenção de ameaças cibernéticas e resposta à incidentes de segurança da informação através da implantação de NOC (Network Operations Center) e SOC (Security Operations Center) na Justiça Federal da 3ª Região – JF3R, conforme especificações e quantitativos estabelecidos no Termo de Referência, (Anexo I - 9122016 do Edital - 9121629), na Proposta Comercial (9286557) e revalidação (9342178) da CONTRATADA.

1.2. Este Termo de Contrato vincula-se ao Edital do Pregão, identificado no preâmbulo, à Proposta Comercial vencedora e à Ata de Registro de Preços nº 12.020.10.2022 (9342827), originária do Processo nº 0024225-52.2022.4.03.8000, independentemente de transcrição.

1.3. Objeto da contratação:

GRUPO 2					
Item	Descrição	Unidade	Quantidade	Valor Unitário (R\$)	Valor Total (R\$)
5	Serviços Gerenciados de Monitoramento de Ambiente Tecnológico e Segurança da Informação – NOC/SOC por 43 (quarenta e três) meses	mês	43	78.000,00	3.354.000,00
Valor Total (R\$)					3.354.000,00

2. CLÁUSULA SEGUNDA – VIGÊNCIA

2.1. O prazo de vigência do presente Contrato inicia-se na data de sua assinatura, prorrogável na forma do art. 57, § 1º, da Lei nº 8.666/1993, conforme segue:

2.1.1. Item 5 do GRUPO 2: vigência de 43 (quarenta e três) meses, compreendendo a prestação mensal de serviços por igual período, contados a partir da assinatura deste Termo de Contrato.

3. CLÁUSULA TERCEIRA – PREÇO

3.1. O valor total da contratação é de R\$ 3.354.000,00 (três milhões trezentos e cinquenta e quatro mil reais), conforme preço unitário discriminado na Proposta Comercial e na tabela da Cláusula Primeira, subitem 1.3.

3.1.1. Os valores estimados para cada exercício são:

3.1.1.1. 2022: R\$ 26.000,00 (vinte e seis mil reais);

3.1.1.2. 2023: R\$ 936.000,00 (novecentos e trinta e seis mil reais);

3.1.1.3. 2024: R\$ 936.000,00 (novecentos e trinta e seis mil reais);

3.1.1.4. 2025: R\$ 936.000,00 (novecentos e trinta e seis mil reais);

3.1.1.5. 2026: R\$ 520.000,00 (quinhentos e vinte mil reais).

3.2. No valor acima estão incluídos todos os custos e as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

3.3. O valor acima é meramente estimativo, de forma que os pagamentos devidos à CONTRATADA dependerão dos quantitativos de serviços efetivamente prestados, nos termos da Proposta Comercial apresentada.

4. CLÁUSULA QUARTA – RECURSOS ORÇAMENTÁRIOS

4.1. As despesas decorrentes da execução deste Contrato correrão por conta do Programa de Trabalho Resumido nº 168443, Fonte de Recurso 0100000000, Natureza da Despesa nº 339040-11 (Suporte de Infraestrutura de TIC), Nota de Empenho nº 2022NE000436 (9358558), emitida em 14/12/2022, pela Unidade Gestora 90029, no valor de R\$ 26.000,00 (vinte e seis mil reais).

4.2. As despesas dos exercícios financeiros seguintes serão empenhadas oportunamente.

5. CLÁUSULA QUINTA – CONDIÇÕES DE FATURAMENTO

5.1. O faturamento do Item 5 do GRUPO 2 será efetuado, mensalmente, após a emissão dos Termo de Recebimento Provisório (conforme Item 5.9.2.1 do Termo de Referência (Anexo I do Edital).

5.2. Os documentos de cobrança serão emitidos em nome do Tribunal Regional Federal da 3ª Região, sem emendas ou rasuras, fazendo menção expressa ao número da Nota de Empenho e contendo todos os dados da mesma e outros, conforme abaixo especificado:

5.2.1. O documento de cobrança deverá ser emitido com o mesmo número de CNPJ constante da documentação apresentada para a habilitação e da Proposta Comercial, o qual serviu de base para a emissão da Nota de Empenho.

5.2.2. Na hipótese de divergência entre o CNPJ do documento de cobrança e o constante na Nota de Empenho, decorrente da necessidade de alteração do estabelecimento comercial emitente durante a execução do Contrato, conforme o caso, a CONTRATADA, deverá apresentar, previamente à emissão do referido documento, declaração justificando a alteração, apresentando ao mesmo tempo, apresentando os comprovantes de regularidade previstos no art. 29, inciso III, da Lei nº 8.666/93, relativos ao estabelecimento comercial emitente.

5.2.3. A justificativa, prevista no subitem anterior, para a alteração do estabelecimento comercial emitente do documento de cobrança, se aceita pela CONTRATANTE, após a análise jurídica, implicará em adequação do Contrato, através de Termo Aditivo, para inclusão do estabelecimento em questão e de seu respectivo CNPJ, bem como para modificação do favorecido dos recursos orçamentários correspondentes.

5.2.4. No caso de alteração, nos termos do subitem anterior, a CONTRATADA deverá apresentar os dados bancários relativos ao CNPJ do estabelecimento responsável pela emissão do documento de cobrança, para que o pagamento possa ser efetuado por meio de ordem bancária.

5.3. No documento de cobrança deverão constar os nomes e os números do banco e da agência, bem como o número da conta corrente à qual se dará o depósito bancário para pagamento, repetindo-se os dados informados na Proposta Comercial.

5.3.1. Qualquer alteração de dados bancários só será permitida desde que efetuada em papel timbrado da empresa, assinada por representante legal e encaminhada ao setor competente da CONTRATANTE (Secretaria de Planejamento, Orçamento e Finanças do TRF3) antes do processamento do respectivo pagamento;

5.4. No documento de cobrança não deverá constar material ou serviço de outra Nota de Empenho.

5.5. Todos os tributos incidentes sobre os produtos ou serviços deverão estar inclusos no valor total do documento de cobrança, observada a legislação tributária aplicável à espécie, principalmente àquela pertinente aos órgãos públicos federais.

5.5.1. Se a CONTRATADA sofrer qualquer uma das retenções dos tributos a seguir elencados: Imposto sobre a Renda da Pessoa Jurídica (IRPJ), Contribuição Social sobre o Lucro Líquido (CSLL), Contribuição para o Financiamento da Seguridade Social (COFINS), Contribuição para o PIS/PASEP (art. 2º, § 6º, da IN RFB nº 1.234/2012) e Contribuição à Previdência Social (artigo 126, da IN RFB nº 971/2009), deverá efetuar o destaque, no respectivo documento de cobrança.

5.6. O documento de cobrança (Nota Fiscal, Fatura, etc.), deverá ser encaminhado ao TRF-3ª REGIÃO por meio do endereço eletrônico **diac@trf3.jus.br** e **ract@trf3.jus.br** ou aos cuidados da Divisão de Aquisições e Acompanhamento de Contratos, situada na Av. Paulista nº 1842, Torre Norte, 19º andar, Quadrante 197, Bela Vista, São Paulo – SP, CEP 01310-945, Telefone (11) 3012-2280 / 3012-1460, que providenciará o protocolo.

5.6.1. Quando do recebimento do documento de cobrança será confirmada a regularidade fiscal e trabalhista da CONTRATADA mediante consulta “on-line” ao Sistema de Cadastramento Unificado de Fornecedores – SICAF, ou na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais referentes à documentação relacionada no Edital e Anexos.

5.6.2. A CONTRATADA deverá manter os documentos mencionados no subitem anterior atualizados durante a vigência do Contrato.

6. CLÁUSULA SEXTA – RETENÇÃO DE IMPOSTOS E CONTRIBUIÇÕES

6.1. Quando do pagamento à CONTRATADA e de acordo com as suas condições específicas, aplicar-se-á, no que couber, o disposto na Lei nº 9.430/1996, Lei nº 8.212/1991 e regulamentação; e Lei Complementar nº 116/2003, combinada com a correspondente Lei Municipal do local de prestação dos serviços, em cotejo com a Lei Municipal do estabelecimento sede da empresa.

6.2. Se a CONTRATADA gozar de tratamento diferenciado em virtude de lei, seja na forma de benefícios ou isenções deverá obrigatoriamente apresentar a comprovação definida no dispositivo legal ou regulamentar que lhe garantiu o direito, sob pena de retenção de tributos na fonte.

6.3. A CONTRATADA optante pelo SIMPLES NACIONAL deverá apresentar no ato da assinatura do contrato, Declaração na forma do Anexo IV da IN RFB nº 1.234/2012, e alterações posteriores, devendo informar imediatamente à CONTRATANTE qualquer alteração da sua permanência no referido regime de arrecadação.

7. CLÁUSULA SÉTIMA – CONDIÇÕES DE PAGAMENTO

7.1. O pagamento será efetuado mediante ordem bancária, nos prazos a seguir indicados, contados da apresentação do regular documento de cobrança, no local e na forma indicada na Cláusula "Condições de Faturamento":

7.1.1. em até 30 (trinta) dias, contados a partir da data final do período de adimplemento do contrato, ou de cada parcela, mediante a apresentação do documento de cobrança, quando o valor total da despesa contratada for superior ao limite estabelecido no art. 24, inciso II, da Lei nº 8.666/1993.

7.1.2. em até 05 (cinco) dias úteis, contados da apresentação do documento de cobrança, quando o pagamento decorrer de despesa cujo valor não ultrapasse o limite estabelecido no art. 24, inc. II, da Lei nº 8.666/1993.

7.2. Havendo erro no documento de cobrança ou circunstância que impeça a liquidação da despesa, aquele será devolvido à CONTRATADA, e o pagamento ficará pendente até que sejam providenciadas as correções. Nesta hipótese, o prazo para pagamento iniciar-se-á após a regularização da situação ou reapresentação do documento de cobrança, não acarretando qualquer ônus para a CONTRATANTE.

7.3. Nos casos de eventuais atrasos de pagamento, desde que a CONTRATADA não tenha concorrido de alguma forma para tanto, fica convencionado que a taxa de atualização financeira devida pela CONTRATANTE, entre a data acima referida e a correspondente ao efetivo adimplemento da parcela, será calculada mediante a aplicação da seguinte fórmula:

$$EM = I \times N \times VP$$

Onde:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela em atraso;

I = Índice de atualização financeira, assim apurado:

$$I = (TX/100)/365 \quad I = (6/100)/365 \quad I = 0,00016438 \text{ ao dia}$$

TX = Percentual da taxa de juros de mora anual = 6%

7.4. O pagamento dos encargos moratórios deverá ser objeto de solicitação da CONTRATADA, não cabendo à Administração fazê-lo de ofício.

8. CLÁUSULA OITAVA – REAJUSTE

8.1. Os preços são fixos e irrevogáveis no prazo de um ano contado da data limite para a apresentação das Propostas.

8.1.1. Dentro do prazo de vigência do Contrato e mediante solicitação da CONTRATADA, o preço contratado poderá sofrer reajuste após o interregno de um ano, aplicando-se o Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

8.1.1.1. A solicitação deve ser encaminhada à Divisão de Aquisições e Acompanhamento de Contratos nos endereços eletrônicos diac@trf3.jus.br e ract@trf3.jus.br.

8.1.2. O encerramento do Contrato ou a sua prorrogação sem a formalização do pedido determinará a preclusão do direito ao reajuste.

8.2. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

8.3. No caso de atraso ou não divulgação do índice de reajustamento, a CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo. Fica a CONTRATADA obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.

8.4. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.

8.5. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.

8.6. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de Termo Aditivo.

8.7. O reajuste será realizado por apostilamento ao presente instrumento.

9. CLÁUSULA NONA – GARANTIA DE EXECUÇÃO

9.1. Não haverá exigência de garantia de execução para a presente contratação.

10. CLÁUSULA DÉCIMA – DA GARANTIA CONTRATUAL DOS SERVIÇOS

10.1. Deverão ser atendidas as condições constantes do subitem 5.3.1 do Termo de Referência (Anexo I do Edital).

11. CLÁUSULA DÉCIMA PRIMEIRA – DO REGIME DE EXECUÇÃO, PRAZOS, LOCAIS E CONDIÇÕES DA PRESTAÇÃO DOS SERVIÇOS

11.1. O regime de execução dos serviços será por empreitada por preço unitário.

11.2. Os prazos de atendimento baseiam-se no tipo de SEVERIDADE, conforme tabela do subitem 5.4.2 do Termo de Referência (Anexo I do Edital).

11.3. O NOC/SOC deve estar disponível em regime integral de 24 (vinte e quatro) horas x 7 (sete) dias na semana e em feriados.

11.4. A CONTRATADA deverá entregar a CONTRATANTE o Relatório de Atividades Interventivas elencando detalhadamente as ações relacionadas a eventos de SEVERIDADE classificados como Médio e Alto ou quaisquer atividades desenvolvidas, bem como a quantidade de horas utilizadas, que impliquem na contratação do ITEM 6 do GRUPO 2, em até 10 (dez) dias corridos, contados a partir da finalização dos serviços realizados.

11.5. Deverão ser atendidos os demais prazos e condições constantes do Termo de Referência (Anexo I do Edital).

12. CLÁUSULA DÉCIMA SEGUNDA – DO RECEBIMENTO DO OBJETO

12.1. O objeto será recebido conforme segue:

12.1.1. Item 5 do GRUPO 2:

12.1.1.1. Provisoriamente: pelo FISCAL DO CONTRATO, mensalmente, mediante termo circunstanciado assinado pelas partes, até o 5º (quinto) dia do mês subsequente ao da prestação mensal dos serviços, mediante aprovação do Relatório Mensal de Atividades.

12.1.1.2. Definitivamente: pelo GESTOR DO CONTRATO, mediante termo circunstanciado, assinado pelas partes, após o decurso do prazo para observação ou vistoria que comprove a adequação do objeto aos termos contratual, não superior a 90 (noventa) dias corridos, conforme art. 73, § 3º, da Lei nº 8.666/93, observado o disposto no art. 69 da mesma.

13. CLÁUSULA DÉCIMA TERCEIRA – OBRIGAÇÕES DA CONTRATANTE

13.1. São obrigações da CONTRATANTE:

13.1.1. exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua Proposta;

13.1.2. exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;

13.1.3. notificar a CONTRATADA por escrito, da ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução dos serviços, fixando prazo para a sua correção, certificando-se que as soluções por ela propostas sejam as mais adequadas;

13.1.4. pagar à CONTRATADA o valor resultante da prestação do serviço, no prazo e condições estabelecidas na Cláusula de Condições de Pagamento;

13.1.5. efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura da CONTRATADA, no que couber, em conformidade com o item 6, do Anexo XI da IN SEGES/MP nº 5/2017;

13.1.6. não praticar atos de ingerência na administração da CONTRATADA, tais como:

13.1.6.1. exercer o poder de mando sobre os empregados da CONTRATADA, devendo reportar-se somente aos prepostos ou responsáveis por ela indicados, exceto quando o objeto da contratação prever o atendimento direto, tais como nos serviços de recepção e apoio ao usuário;

13.1.6.2. direcionar a contratação de pessoas para trabalhar nas empresas contratadas;

13.1.6.3. promover ou aceitar o desvio de funções dos trabalhadores da CONTRATADA, mediante a utilização destes em atividades distintas daquelas previstas no objeto da contratação e em relação à função específica para a qual o trabalhador foi contratado; e

13.1.6.4. considerar os trabalhadores da CONTRATADA como colaboradores eventuais do próprio órgão ou entidade responsável pela contratação, especialmente para efeito de concessão de diárias e passagens.

13.1.7. fornecer por escrito as informações necessárias para o desenvolvimento dos serviços objeto do Contrato;

13.1.8. realizar avaliações periódicas da qualidade dos serviços, após seu recebimento;

13.1.9. cientificar o órgão de representação judicial da Advocacia-Geral da União para adoção das medidas cabíveis quando do descumprimento das obrigações pela CONTRATADA;

13.1.10. arquivar, entre outros documentos, projetos, "as built", especificações técnicas, orçamentos, termos de recebimento, contratos e aditamentos, relatórios de inspeções técnicas após o recebimento do serviço e notificações expedidas;

13.1.11. fiscalizar o cumprimento dos requisitos legais, quando a CONTRATADA houver se beneficiado da preferência estabelecida pelo art. 3º, § 5º, da Lei nº 8.666/1993.

13.2. Atender as demais condições do subitem 2.12 do Termo de Referência.

14. CLÁUSULA DÉCIMA QUARTA – OBRIGAÇÕES DA CONTRATADA

14.1. São obrigações da CONTRATADA:

14.1.1. executar os serviços conforme especificações do Termo de Referência e de sua Proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, além de fornecer e utilizar os materiais e equipamentos, ferramentas e utensílios necessários, na qualidade e quantidade mínimas especificadas no Termo de Referência e em sua Proposta;

14.1.2. reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do Contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

14.1.3. responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado, devendo ressarcir imediatamente a Administração em sua integralidade, ficando a CONTRATANTE autorizada a descontar da garantia, caso exigida no Edital, ou dos pagamentos devidos à CONTRATADA, o valor correspondente aos danos sofridos, observado o art. 70 da Lei nº 8.666/1993, sem prejuízo da ampla defesa e do contraditório;

14.1.4. utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor;

14.1.5. indicar preposto para representá-la durante a execução do Contrato no prazo definido no Termo de Referência;

14.1.6. vedar a utilização, na execução dos serviços, de empregados que sejam cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de ocupantes de cargos de direção e assessoramento de membros ou juízes vinculados à CONTRATANTE, conforme art. 3º da Resolução nº 007/2005, do Conselho Nacional de Justiça, e suas alterações posteriores;

14.1.7. quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, entregar ao setor responsável pela fiscalização do Contrato, até o dia 30 (trinta) do mês seguinte ao da prestação dos serviços, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda Municipal ou Distrital do domicílio ou sede do contratado; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT, conforme item 10.2, alínea "c", do Anexo VIII-B da IN SEGES/MP nº 5/2017;

14.1.8. responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo Contrato, por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade à CONTRATANTE;

- 14.1.9. comunicar ao fiscal do Contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços;
- 14.1.10. prestar todo esclarecimento ou informação solicitada pela CONTRATANTE ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do empreendimento;
- 14.1.11. paralisar, por determinação da CONTRATANTE, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros;
- 14.1.12. promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução dos serviços, durante a vigência do Contrato;
- 14.1.13. promover a organização técnica e administrativa dos serviços, de modo a conduzi-los eficaz e eficientemente, de acordo com os documentos e especificações que integram o Termo de Referência, no prazo determinado;
- 14.1.14. conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina;
- 14.1.15. submeter previamente, por escrito, à CONTRATANTE, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do Termo de Referência;
- 14.1.16. não permitir a utilização de qualquer trabalho do menor de 16 (dezesesseis) anos, exceto na condição de aprendiz para os maiores de 14 (quatorze) anos; nem permitir a utilização do trabalho do menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre;
- 14.1.17. manter durante toda a vigência do Contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;
- 14.1.18. cumprir, durante todo o período de execução do Contrato, a reserva de cargos prevista em Lei para pessoa com deficiência ou para reabilitado da Previdência Social, bem como as regras de acessibilidade previstas na legislação, quando a CONTRATADA houver se beneficiado da preferência estabelecida pela Lei nº 13.146/2015;
- 14.1.19. guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do Contrato;
- 14.1.20. arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua Proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, tais como os valores providos com o quantitativo de vale-transporte, devendo complementá-los, caso o previsto inicialmente em sua Proposta não seja satisfatório para o atendimento do objeto da licitação, exceto quando ocorrer algum dos eventos arrolados no art. 57, § 1º, da Lei nº 8.666/1993;
- 14.1.21. cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança, higiene e saúde da CONTRATANTE;
- 14.1.22. prestar os serviços dentro dos parâmetros e rotinas estabelecidos, fornecendo todos os materiais, equipamentos e utensílios em quantidade, qualidade e tecnologia adequadas, com a observância às recomendações aceitas pela boa técnica, normas e legislação.

15. CLÁUSULA DÉCIMA QUINTA – GERENCIAMENTO E FISCALIZAÇÃO

- 15.1. O gerenciamento desta contratação será efetuado pela Divisão de Atendimento de Redes - DRED, sendo a fiscalização realizada pelo(s) servidor(es) ou seu(s) substituto(s) especialmente designado(s) pela autoridade competente, mediante Portaria, em conformidade com o disposto no art. 67 da Lei nº 8.666/1993.
- 15.2. Nos termos do art. 67 da Lei nº 8.666/1993, o fiscal anotará em registro próprio todas as ocorrências relacionadas com a execução e determinará o que for necessário à regularização de falhas ou defeitos observados, encaminhando os apontamentos à autoridade competente para as providências cabíveis.
- 15.3. A omissão, total ou parcial, da fiscalização não eximirá a CONTRATADA da integral responsabilidade pelos encargos ou serviços que são de sua competência.
- 15.4. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e, na ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos, em conformidade com o art. 70 da Lei nº 8.666/1993.

16. CLÁUSULA DÉCIMA SEXTA – SANÇÕES ADMINISTRATIVAS

- 16.1. Na aplicação das penalidades devem ser consideradas as seguintes circunstâncias:

- a) a natureza e a gravidade da infração contratual;
- b) os danos que o cometimento da infração ocasionar ao serviço e a terceiros;
- c) a vantagem auferida em virtude da infração;
- d) as circunstâncias gerais agravantes e atenuantes; e
- e) os antecedentes da CONTRATADA.

- 16.2. Na inexecução parcial ou total do Contrato, sempre por circunstância que lhe seja imputável, a CONTRATADA estará sujeita à aplicação das seguintes penalidades, garantida a prévia defesa, em conformidade com os art. 86 e 87 da Lei nº 8.666/1993 ou com o art. 7º da Lei nº 10.520/2002:

- a) advertência;
- b) multa moratória, excluída a hipótese prevista no subitem 5.4.2.2. do Termo de Referência (SLA mensal), de:
 - b.1) 0,2% (dois décimos por cento) ao dia, limitada a 3% (três por cento), sobre o valor do atualizado do Contrato ou da parcela inadimplida, na demora injustificada para o cumprimento da obrigação ou para a correção da entrega do produto, após ser devolvido ou recusado por não atender às especificações do Edital, pelo prazo de até 15 (quinze) dias;
 - b.2) 0,3% (três décimos por cento) ao dia, limitada a 7,5% (sete e meio por cento) sobre o valor atualizado do Contrato ou da parcela inadimplida, na demora injustificada para o cumprimento da obrigação ou para a correção da entrega do produto, após ser devolvido ou recusado por não atender às especificações do Edital e seus Anexos, pelo prazo de até 25 (vinte e cinco) dias;

c) multa compensatória de até 10% (dez por cento) sobre o valor atualizado do Contrato ou da parcela inadimplida, em casos de atraso superior a 25 (vinte e cinco) dias e, também, por ocorrência não prevista na presente cláusula e que descumpra quaisquer dos itens do Edital e seus Anexos, casos em que a Administração poderá aceitar ou rejeitar o bem e, se entender conveniente, formalizar a rescisão unilateral do Contrato, conforme dispõe o art. 78, inc. I e II, da Lei nº 8.666/1993;

d) multa compensatória de até 10% (dez por cento) sobre o valor total atualizado do Contrato, em caso de descumprimento total da obrigação assumida;

e) suspensão temporária do direito de licitar e de contratar com TRF-3ª REGIÃO, pelo prazo fixado pela CONTRATANTE, em conformidade com a natureza e a gravidade da falta, respeitado o limite de 02 (dois) anos, sem prejuízo da aplicação das multas previstas em Edital e no Contrato e das demais cominações legais;

f) declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a CONTRATADA ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base na alínea anterior;

g) impedimento de licitar e de contratar com a União e descredenciamento no SICAF pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas em Edital e no Contrato e das demais cominações legais.

16.2.1. a CONTRATADA estará sujeita à multa por reincidência em advertência e às sanções aplicáveis aos itens 5 e 6 do GRUPO 2, pelo descumprimento no SLA mensal, conforme subitens 6.1 e 6.2 do Termo de Referência.

16.3. Em caso de apuração de falta contratual, o valor da multa aplicada será:

16.3.1. retido dos pagamentos devidos pela Administração, após regular procedimento de apuração de falta contratual;

16.3.2. pago por meio de Guia de Recolhimento da União – GRU;

16.3.3. descontado do valor da garantia prestada, quando houver; ou

16.3.4. cobrado judicialmente.

16.4. Para determinar a reincidência, serão considerados os antecedentes da CONTRATADA durante a vigência desta contratação, devendo o descumprimento se referir a uma mesma obrigação contratual.

16.4.1. Caracterizada a reincidência, o valor da multa será majorado em até 1/3 (um terço), levando-se em consideração o número de reiterações e sua gravidade.

16.5. No caso de a infração causar prejuízo a esta Administração, e este prejuízo exceder o valor da multa compensatória, a Administração poderá exigir indenização suplementar. Nessa situação a sanção de multa valerá como princípio de pagamento, competindo à Administração provar o prejuízo.

16.6. No caso de não recolhimento do valor da multa por GRU, dentro do prazo de 5 (cinco) dias úteis, contados da data da intimação, a importância será descontada da garantia prestada ou cobrada judicialmente, consoante o art. 86, § 3º, e o art. 87, § 1º, da Lei nº 8.666/1993.

16.7. As sanções de advertência, suspensão temporária do direito de licitar e de contratar com a Unidade Gestora (TRF-3ª REGIÃO), impedimento para licitar e contratar com a União e a declaração de inidoneidade para licitar ou contratar com a Administração Pública poderão ser aplicadas à CONTRATADA juntamente com a de multa.

16.8. Se o descumprimento consistir na perda das condições de habilitação, a Administração concederá o prazo de 30 (trinta) dias para a empresa regularizar a sua situação, sem cominação de penalidade para o período.

16.8.1. Não regularizando sua situação no prazo de 30 (trinta) dias, poderá ser aplicada a penalidade de multa à empresa no importe de 1% (um por cento) ao dia, sobre o valor atualizado do Contrato ou sobre a parcela entregue e pendente de regularização, limitada a 10% (dez por cento) sobre o valor total atualizado do Contrato e, a critério da Administração, o Contrato poderá ser rescindido.

16.9. A atualização de valores, para efeito de aplicação de multa, será efetivada com base na variação do IPCA-E/IBGE, apurada a partir do mês correspondente à data limite para a apresentação da Proposta Comercial até o mês imediatamente anterior à ocorrência do fato.

16.10. As penalidades previstas neste Contrato não poderão ser relevadas, salvo quando ficar comprovada a ocorrência de situações que se enquadrem no conceito jurídico de força maior, caso fortuito ou outro justo motivo reconhecido pela Administração.

16.11. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto na Lei nº 8.666/1993 e na Lei nº 9.784/1999.

16.12. As penalidades aplicadas à CONTRATADA, após regular procedimento de apuração de falta, serão registradas no SICAF e no CEIS.

17. CLÁUSULA DÉCIMA SÉTIMA – RESCISÃO

17.1. O presente Termo de Contrato poderá ser rescindido:

17.1.1. por ato unilateral e escrito da Administração, nas situações previstas no art. 78, inc. I a XII e XVII, da Lei nº 8.666/1993, e com as consequências indicadas no art. 80 da mesma Lei, sem prejuízo da aplicação das sanções previstas neste Contrato;

17.1.2. amigavelmente, nos termos do art. 79, inc. II, da Lei nº 8.666/1993.

17.2. Os casos de rescisão contratual serão formalmente motivados, assegurando-se à CONTRATADA o direito à prévia e ampla defesa.

17.3. Constitui motivo de rescisão contratual a contratação de empregados que sejam cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de ocupantes de cargos de direção e de assessoramento, de membros ou juízes vinculados à respectiva CONTRATANTE, conforme art. 3º da Resolução nº 007/2005, do Conselho Nacional de Justiça, e suas alterações posteriores.

17.4. A CONTRATADA reconhece os direitos da CONTRATANTE em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666/1993.

17.5. O termo de rescisão será precedido de Relatório indicativo dos seguintes aspectos, conforme o caso:

17.5.1. balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

17.5.2. relação dos pagamentos já efetuados e ainda devidos;

17.5.3. indenizações e multas.

18. CLÁUSULA DÉCIMA OITAVA – VEDAÇÕES E PERMISSÕES

18.1. É vedado à CONTRATADA interromper a execução dos serviços sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.

19. CLÁUSULA DÉCIMA NONA – ALTERAÇÕES

19.1. Eventuais alterações contratuais rege-se-ão pela disciplina do art. 65 da Lei nº 8.666/1993.

19.2. A CONTRATADA é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do Contrato.

19.3. As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do Contrato.

20. CLÁUSULA VIGÉSIMA – DOS CASOS OMISSOS

20.1. Os casos omissos serão decididos pela CONTRATANTE, segundo as disposições contidas na Lei nº 8.666/1993, na Lei nº 10.520/2002 e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078/1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

21. CLÁUSULA VIGÉSIMA PRIMEIRA – PUBLICAÇÃO

21.1. Incumbirá à CONTRATANTE providenciar a publicação deste instrumento, por extrato, no Diário Oficial da União, no prazo previsto na Lei nº 8.666/1993, bem como no Diário Eletrônico da Justiça Federal da 3ª Região, sendo sua eficácia condicionada às publicações, em cumprimento ao que dispõe o art. 61, parágrafo único, da Lei nº 8.666/1993.

22. CLÁUSULA VIGÉSIMA SEGUNDA – COMUNICAÇÕES

22.1. Eventuais correspondências expedidas pelas partes signatárias deverão mencionar o número deste instrumento e o assunto específico da correspondência.

22.1.1. As comunicações feitas ao TRIBUNAL REGIONAL FEDERAL DA 3ª REGIÃO, deverão ser endereçadas à Divisão de Administração de Redes (DRED) situada na Av. Paulista nº 1.842, Torre Norte, 19º andar, Bela Vista, São Paulo – SP, CEP 01310-945, Telefone (11) 3012-2280 / 3012-1460 ou pelo e-mail dred@trf3.jus.br.

22.1.2. As comunicações feitas pelo TRIBUNAL REGIONAL FEDERAL DA 3ª REGIÃO, em decorrência desta contratação ou de eventuais processos administrativos a ela inerentes, inclusive as relativas ao informe de rendimentos anual (conforme previsão contida no art. 37 da IN RFB nº 1.234/2012, em se tratando de pessoa jurídica, e no art. 3º, § 3º, da IN RFB nº 2.060/2021, no caso de pessoa física), serão realizadas em regra, por via eletrônica, no e-mail adriano.moreira@s3curity.com.br, conforme informado na Proposta Comercial, devendo a FORNECEDORA mantê-la atualizada.

22.1.3. À CONTRATADA caberá confirmar o recebimento da correspondência eletrônica, no prazo de 1 (um) dia útil, contado de seu envio pela CONTRATANTE.

22.1.3.1. Na hipótese de ausência de confirmação do recebimento da correspondência eletrônica no prazo acima estipulado, considerar-se-á como realizada e recebida a comunicação pela CONTRATADA.

22.1.4. Nos prazos para apresentação de defesa prévia e recurso, a Seção responsável pela intimação da CONTRATADA, franqueará, independentemente de pedido expresso, acesso ao “SEI – Sistema Eletrônico de Informações” ao representante legal da CONTRATADA, cujos dados foram informados na Proposta Comercial.

22.1.5. Quando estritamente necessário, as comunicações serão enviadas por via postal, endereçadas à empresa **S3SECURITY TECNOLOGIA SERVIÇOS DE INFORMÁTICA LTDA**, situada na Rua da Conceição nº 188, sala 2801A, Centro, Niterói – RJ, CEP 24020-087, telefone (11) 4063-3434.

22.1.5.1. No caso de intimação para defesa e/ou recurso enviada por via postal e tratando-se de endereço localizado em edifício comercial, a CONTRATADA está ciente que a intimação será entregue na portaria e que o prazo para resposta será contado a partir do recebimento por funcionário próprio ou terceirizado atuante na referida portaria.

22.1.6. Eventuais mudanças de endereços deverão ser comunicadas por escrito.

23. CLÁUSULA VIGÉSIMA TERCEIRA – FORO

23.1. O Foro para solucionar os litígios que decorrerem da execução deste Termo de Contrato será o da Justiça Federal de Primeiro Grau em São Paulo - 1ª Subseção Judiciária.

Assim, por estarem as partes devidamente ajustadas, assinam o presente Termo de Contrato.



Documento assinado eletronicamente por **Ana Lúcia Caurel, Assessora de Licitações e Contratos**, em 15/12/2022, às 21:30, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **ELESSANDRO DA SILVA MOREIRA, Usuário Externo**, em 16/12/2022, às 12:08, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **Marisa Ferreira dos Santos, Desembargadora Federal Presidente**, em 16/12/2022, às 13:29, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site http://sei.trf3.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **9361756** e o código CRC **80B2F35A**.

PLANILHA DE COMPOSIÇÃO DO PREÇO DE REFERÊNCIA

PREGÃO ELETRÔNICO Nº 001/2023

Objeto: O objeto da presente licitação é a seleção da proposta mais vantajosa para a contratação de empresa especializada em SERVIÇOS GERENCIADOS DE SEGURANÇA, durante o período de 60 (sessenta) meses.

Contratações da Administração Pública				
CONTRATANTE	CONSELHO FEDERAL DE CONTABILIDADE	CONSELHO REGIONAL DE CONTABILIDADE DO ESTADO DE SÃO PAULO	TRIBUNAL REGIONAL DO TRABALHO DA 17.ª REGIÃO	TRIBUNAL REGIONAL FEDERAL DA 3ª REGIÃO
CONTRATADA	ISH TECNOLOGIA S/A	ISH TECNOLOGIA S/A	INTELLIWAY TECNOLOGIA LTDA	S3CURITY TECNOLOGIA SERVIÇOS DE INFORMÁTICA LTDA
PREÇO MENSAL	R\$ 14.537,50	R\$ 35.500,00	R\$ 101.825,00	R\$ 78.000,00

Verificação do preços estimado mensal de acordo com as metodologias estabelecidas na Instrução Normativa 73/2020 - Seges		
Média	Mediana	Menor Preço
R\$ 57.465,63	R\$ 56.750,0000	R\$ 14.537,50

Observação: Conforme disposto na Instrução Normativa nº 73/2020 - Seges, feita a análise entre as metodologias previstas, considera-se como mais vantajosa para a Administração, a que refere ao "menor preço"; tendo em vista, ainda, que as especificações técnicas dos serviços, objeto do contrato celebrado pelo Conselho Federal de Contabilidade (CFC), possuem estreita similaridade com as da solução que o CRCMG pretende contratar, conforme descrito no Termo de Referência.

Cumprir registrar que, a contratação do CFC é constituída de 2 itens, sendo: Item 1: Serviço de Suporte Técnico com Monitoramento de ativos 24x7 e Operação Remota (Centro de Operação Remoto. Item 2: Analista de TI para a prestação de serviços técnicos de Administração, Suporte e Operação de Rede de Dados Local. Considerando que os serviços também foram precificados em separado, tomou-se como balizamento de preços apenas os serviços referentes ao item 1, que guarda semelhança com a contratação de que trata esta composição de valor de referência.

Dessa forma, adotando-se o menor preço como metodologia, o valor estimado global da contratação, durante o período de 60 (sessenta) meses, corresponderá ao montante de R\$ 872.250,00 (oitocentos e setenta e dois mil duzentos e cinquenta reais).

Valor de Referência	
Parâmetro	Contratações da Administração Pública
Metodologia	Menor Preço
Valor mensal	R\$ 14.537,50
Valor global anual	R\$ 174.450,00
Valor global 60 meses	R\$ 872.250,00

Assinado digitalmente por:
CLAUDIO MARCIO ARAUJO DA SILVA
CPF: 691.116.426-53
Este documento foi assinado por CLAUDIO MARCIO ARAUJO DA SILVA
Certificado emitido por AC SOLUTI Multipla v5
Data: 19/01/2023 17:44:09 -03:00

Assinado digitalmente por:
JULIO CESAR DA SILVA
CPF: 890.313.705-64
Este documento foi assinado por JULIO CESAR DA SILVA
Certificado emitido por AC SOLUTI Multipla v5
Data: 19/01/2023 17:44:09 -03:00

Assinado digitalmente por:
SUELY MARIA MARQUES DE OLIVEIRA
CPF: 890.313.705-64
Este documento foi assinado por SUELY MARIA MARQUES DE OLIVEIRA
Certificado emitido por AC SOLUTI Multipla v5
Data: 20/01/2023 08:04:52 -03:00

Gerente de Tecnologia da
Informação

Diretor-Adjunto de Gestão
Operacional

Presidente do CRCMG



MANIFESTO DE ASSINATURAS



Código de validação: 3RL57-KZT7W-QA5Z8-BX4HV

Esse documento foi assinado pelos seguintes signatários nas datas indicadas (Fuso horário de Brasília):

- ✓ CLAUDIO MARCIO ARAUJO DA SILVA (CPF 691.116.426-53) em 19/01/2023 14:50 - Assinado com certificado digital ICP-Brasil
- ✓ JULIO CESAR DA SILVA (CPF 890.312.706-44) em 19/01/2023 17:44 - Assinado com certificado digital ICP-Brasil
- ✓ SUELY MARIA MARQUES DE OLIVEIRA (CPF 686.588.426-49) em 20/01/2023 08:04 - Assinado com certificado digital ICP-Brasil

Para verificar as assinaturas, acesse o link direto de validação deste documento:

<https://assinador.crcmg.org.br/validate/3RL57-KZT7W-QA5Z8-BX4HV>

Ou acesse a consulta de documentos assinados disponível no link abaixo e informe o código de validação:

<https://assinador.crcmg.org.br/validate>

Número da Reserva	Ano do Exercício	Data da Reserva	Processo
208	2023	19.01.2023	

Conta de Despesa	Descrição da Conta	Projeto	SubProjeto
6.3.1.3.02.01.005	SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO	5002-TECNOLOGIA DA	-

Histórico da Reserva	Valor Total da Reserva
CONTRATAÇÃO DE EMPRESA ESPECIALIZADA EM SERVIÇOS GERENCIADOS DE SEGURANÇA, CONSTITUÍDO DE SERVIÇOS DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS E RESPOSTA A INCIDENTES; SERVIÇOS DE GESTÃO DE VULNERABILIDADES; SERVIÇO DE MONITORAMENTO, DETECÇÃO E RESPOSTA A INCIDENTES PARA ENDPOINTS. PERÍODO DE FEVEREIRO/2023 A DEZEMBRO/2023.	159.912,50

Valor por Extenso
Cento e Cinquenta e Nove Mil, Novecentos e Doze Reais e Cinquenta Centavos

Dotação Atualizada	Reservas Acumuladas	Valor desta Reserva	Saldo Atual
1.228.100,00	652.293,29	159.912,50	415.894,21

Belo Horizonte, 19 de Janeiro de 2023

Assinado digitalmente por:
JULIO CESAR DA SILVA
CPF: 890.312.706-44
Certificado emitido por AC SOLUTI Multipla v5
Data: 20/01/2023 08:19:33 -03:00

Assinado digitalmente por:
MARIO ROGERIO MAROTTA
CPF: 269.729.056-72
Certificado emitido por AC SAFEWEB RFB v5
Data: 20/01/2023 09:17:30 -03:00

Assinado digitalmente por:
SUELY MARIA MARQUES DE OLIVEIRA
CPF: 686.588.426-49
Certificado emitido por AC SOLUTI Multipla v5
Data: 20/01/2023 09:17:59 -03:00



MANIFESTO DE ASSINATURAS



Código de validação: A8HVU-GNUHJ-ETMWX-YC22W

Esse documento foi assinado pelos seguintes signatários nas datas indicadas (Fuso horário de Brasília):

- ✓ JULIO CESAR DA SILVA (CPF 890.312.706-44) em 20/01/2023 08:19 -
Assinado com certificado digital ICP-Brasil
- ✓ MARIO ROGERIO MAROTTA (CPF 269.729.056-72) em 20/01/2023 09:17 -
Assinado com certificado digital ICP-Brasil
- ✓ SUELY MARIA MARQUES DE OLIVEIRA (CPF 686.588.426-49) em 20/01/2023
09:17 - Assinado com certificado digital ICP-Brasil

Para verificar as assinaturas, acesse o link direto de validação deste documento:

<https://assinador.crcmg.org.br/validate/A8HVU-GNUHJ-ETMWX-YC22W>

Ou acesse a consulta de documentos assinados disponível no link abaixo e informe o código de validação:

<https://assinador.crcmg.org.br/validate>



**SOLICITAÇÃO / AUTORIZAÇÃO
ABERTURA DE PROCESSO DE CONTRATAÇÃO**

OBJETO	Contratação de empresa especializada em SERVIÇOS GERENCIADOS DE SEGURANÇA.
SETOR SOLICITANTE	Gerência de Tecnologia da Informação
JUSTIFICATIVA	Considerando que nos últimos anos temos visto diversas instituições públicas e privadas sofrendo constantes ataques cibernéticos, e tendo em vista a implantação da LGPD no CRCMG, que exige a adoção de medidas de segurança mais eficazes, torna-se indispensável a aplicação de boas práticas de segurança da informação no ambiente tecnológico do CRCMG, a fim de torna-lo mais seguro e menos suscetível a esses ataques. Diante do crescimento exponencial de ameaças e ataques sofridos a empresas privadas e órgãos públicos no Brasil e no mundo, investimentos contínuos em segurança da informação são fundamentais para a mitigação de riscos de segurança associados ao negócio de maneira a resguardar a confidencialidade, a disponibilidade e a integridade das informações. O cenário de ameaças à segurança da informação não se resume somente em ataques aos serviços de TI pela Internet. Tentativas de acesso não autorizado, infecção por arquivos maliciosos (vírus), e-mails indesejados (SPAMs), engenharia social, entre outros, são exemplos de eventos que podem apresentar riscos à segurança de TI. Até mesmo colaboradores não conscientes ou mal-intencionados representam risco potencial à segurança da informação. Na busca de aperfeiçoamento da sua missão institucional e gestão pública, o Conselho Regional de Contabilidade de Minas Gerais vem utilizando cada vez mais soluções de TI, disponibilizando aos seus colaboradores, profissionais contábeis e à sociedade diversos serviços relacionados à Tecnologia da Informação. Nesse cenário, diversas foram as mudanças: tanto em termos de quantidade de serviços oferecidos quanto em diversidade de soluções, o que contribui para o aumento dos riscos e da necessidade de monitoramento, à medida que cresce a oferta de serviços pela Internet. Nesse sentido, incidentes de segurança da informação, como nas hipóteses de violação, roubo ou perda de informações custodiadas pelo CRCMG, podem constituir possíveis situações capazes de inviabilizar, senão a totalidade, parte das atividades desta Entidade. Assim, a ocorrência de eventuais sinistros poderia provocar o vazamento de informações e prejuízo à sua imagem, podendo ainda o Conselho ter que responder pelos danos causados. Por esses motivos, e devido ao incidente ocorrido recentemente no ambiente, tendo em vista que o Conselho não dispõe de infraestrutura física

PE-002/AF
4/10/2018

	e pessoal para o monitoramento e gerenciamento de dispositivos de segurança com diversos fornecedores (firewall, sistema de prevenção de intrusões de rede, gerenciamento unificado de ameaças), capazes de realizar ações contra incidentes de segurança de forma tempestiva e procedimental, torna-se necessária realizar a contratação de uma solução que forneça uma estrutura em segurança da informação adequada, de forma a propiciar a integridade, confidencialidade, autenticidade e a disponibilidade dos dados, através de um monitoramento preventivo e contínuo de segurança da informação contra ataques cibernéticos e de serviço de resposta a incidentes de segurança. A contratação pretendida está alinhada com o planejamento estratégico do CRCMG, uma vez que contribuirá para o alcance do objetivo da qualidade de “Assegurar meios e recursos que permitam o cumprimento das políticas e diretrizes da gestão”, bem como dos objetivos estratégicos de “garantir qualidade e confiabilidade nos processos e nos procedimentos” e “Assegurar adequada infraestrutura e suporte logístico às necessidades dos CRCs”.
VALOR ESTIMADO	O valor de referência para a prestação dos serviços, durante o período de 60 (sessenta) meses é de R\$ 872.250,00 (oitocentos e setenta e dois mil e duzentos e cinquenta reais).

Belo Horizonte, 23 de janeiro de 2023

Assinado digitalmente por:
 CLAUDIO MARCIO ARAUJO DA SILVA
 CPF: 691.116.426-53
 Certificado emitido por AC SOLUTI Multipla
 Data: 23/01/2023 11:03:58 -03:00



Cláudio Márcio Araújo da Silva
 Gerente de Tecnologia da Informação

Assinado digitalmente por:
 MARIA APARECIDA LOPES MONTEIRO CARDOSO
 CPF: 994.036.416-49
 Certificado emitido por AC CERTIFICA MINAS v5
 Data: 23/01/2023 11:04:34 -03:00



Maria Aparecida Lopes Monteiro Cardoso
 Diretora Adjunta de Gestão de Recursos

Autorizo a abertura do respectivo processo, respeitando a legislação vigente e demais normas aplicáveis à espécie.

Assinado digitalmente por:
 SUELY MARIA MARQUES DE OLIVEIRA
 CPF: 686.588.426-49
 Certificado emitido por AC SOLUTI Multipla v5
 Data: 23/01/2023 14:15:38 -03:00



Suely Maria Marques de Oliveira
 Presidente

PE-002/AF
 4/10/2018



MANIFESTO DE ASSINATURAS



Código de validação: SPPBS-XHG8D-T9HAL-DESKN

Esse documento foi assinado pelos seguintes signatários nas datas indicadas (Fuso horário de Brasília):

- ✓ CLAUDIO MARCIO ARAUJO DA SILVA (CPF 691.116.426-53) em 23/01/2023 11:03 - Assinado com certificado digital ICP-Brasil
- ✓ MARIA APARECIDA LOPES MONTEIRO CARDOSO (CPF 994.036.416-49) em 23/01/2023 11:04 - Assinado com certificado digital ICP-Brasil
- ✓ SUELY MARIA MARQUES DE OLIVEIRA (CPF 686.588.426-49) em 23/01/2023 14:15 - Assinado com certificado digital ICP-Brasil

Para verificar as assinaturas, acesse o link direto de validação deste documento:

<https://assinador.crcmg.org.br/validate/SPPBS-XHG8D-T9HAL-DESKN>

Ou acesse a consulta de documentos assinados disponível no link abaixo e informe o código de validação:

<https://assinador.crcmg.org.br/validate>

PORTARIA CRCMG N.º 137, DE 4 DE AGOSTO DE 2022.

Designa membros da Comissão Permanente de Licitação, Pregoeiros e Equipe de Apoio do CRCMG e define procedimentos de controle.

A PRESIDENTE DO CONSELHO REGIONAL DE CONTABILIDADE DE MINAS GERAIS, no uso de suas atribuições legais e regimentais,

R E S O L V E:

Art. 1º Ficam designados como membros efetivos da Comissão Permanente de Licitação (CPL) do CRCMG, nos termos dos §§ 2º, 3º e 4º do artigo 51 da Lei n.º 8.666/1993, os seguintes funcionários:

I - Sérgio Robson Mafra - funcionário efetivo, ocupante do cargo de Contador, portador da matrícula n.º 502, com qualificação técnica comprovada em licitações públicas, conforme consta em sua pasta funcional;

II - Maria Christina de Oliveira - funcionária efetiva, ocupante do cargo de Advogada, portadora da matrícula n.º 526, com qualificação técnica comprovada em licitações públicas, conforme consta em sua pasta funcional;

III - Suélen Teixeira de Paula - funcionária efetiva, ocupante do cargo de Auxiliar Administrativo, portadora da matrícula n.º 513, com qualificação técnica comprovada em licitações públicas, conforme consta em sua pasta funcional.

Parágrafo único. Ficam designados como Presidente e Secretário da Comissão os funcionários indicados nos incisos I e II, respectivamente.

Art. 2º Em casos de faltas e impedimentos temporários, os membros efetivos serão substituídos pelos suplentes:

I - Otacílio Valadares Cordeiro - funcionário efetivo, ocupante do cargo de Advogado, portador da matrícula n.º 498, com qualificação técnica comprovada em licitações públicas, conforme consta em sua pasta funcional;

II - Ricardo Andrade Tonaco - funcionário efetivo, ocupante do cargo de Fiscal, portador da matrícula n.º 327, com qualificação técnica comprovada em licitações públicas, conforme consta em sua pasta funcional.

III - Robson Barbosa Miranda - funcionário efetivo, ocupante do cargo de Fiscal, portador da matrícula n.º 492, com qualificação técnica comprovada em licitações públicas, conforme consta em sua pasta funcional.

Art. 3º A Comissão Permanente de Licitação do CRCMG atuará na fase externa da licitação, tendo como atribuição: responder pedidos de esclarecimentos; julgar pedidos de impugnação; conduzir as sessões públicas e julgar preliminarmente a habilitação, as propostas, os recursos e demais questionamentos sobre os processos administrativos de licitação pública.

§ 1º A comissão designada terá como quórum para iniciar qualquer sessão o número mínimo de três membros nomeados por esta portaria.

§ 2º Durante as sessões, a Comissão Permanente de Licitação poderá contar com a presença do Controlador Interno do CRCMG, com direito a voz, mas sem direito a voto, com poderes para questionar, determinar e reprimir atos abusivos ou considerados em desacordo com a legislação, requerer a suspensão das sessões ou vista dos autos, devendo suas manifestações serem registradas nos autos do processo.

§ 3º Em decorrência do exame dos autos, nos termos do § 2º do artigo 113 da Lei n.º 8.666/1993, o Controle Interno do CRCMG poderá emitir pareceres, como ato de regularidade ou de determinação, para adoção de medidas corretivas pertinentes.

Art. 4º Poderão ser convocados para integrar a Comissão Permanente de Licitação, em determinadas sessões, profissionais com qualificação técnica em áreas específicas, especialmente nos seguintes casos:

I - em licitação de obras, reforma e demolições, o engenheiro ou arquiteto pertencente ao quadro do CRCMG ou, na ausência deste, profissional contratado;

II - em licitação de tecnologia da informação e outros objetos que demandem conhecimentos técnicos específicos, os responsáveis técnicos pertencentes ao quadro efetivo do CRCMG ou profissionais contratados, responsáveis pela descrição técnica dos materiais e serviços.

Art. 5º Ficam designados como pregoeiros oficiais do CRCMG, para atuarem nos processos administrativos de licitação na modalidade Pregão, os seguintes funcionários:

- I - Sérgio Robson Mafra, já qualificado acima;
- II - Maria Christina de Oliveira, já qualificada acima;
- III - Suélen Teixeira de Paula, já qualificada acima.

§ 1º Os pregoeiros acima designados possuem qualificação técnica comprovada e conhecimento notório em licitações públicas, conforme consta em suas pastas funcionais.

§ 2º Os pregoeiros serão convocados individualmente pela Gerência Administrativa e Financeira para atuarem na fase externa do Pregão, conforme disponibilidade dos funcionários.

Art. 6º Os pregoeiros atuarão na fase externa do pregão, tendo como atribuição: responder pedidos de esclarecimentos; julgar pedidos de impugnação; conduzir a etapa de lances e julgar a habilitação, as propostas, os recursos e demais questionamentos sobre os processos administrativos de licitação pública na modalidade Pregão.

Art. 7º Ficam designados para compor a equipe de apoio na modalidade de licitação Pregão os seguintes funcionários:

I – Otacílio Valadares Cordeiro, já qualificado acima;
II – Ricardo Andrade Tonaco, já qualificado acima;
III – Robson Barbosa Miranda, já qualificado acima;
IV – Andreza Maia Bitarães - funcionária efetiva, ocupante do cargo de Auxiliar Administrativo, portadora da matrícula n.º 363, com qualificação técnica comprovada em licitações públicas, conforme consta em sua pasta funcional.

Parágrafo único. O Pregoeiro poderá dispensar a equipe de apoio quando julgar-se competente para conduzir o certame sozinho, sem prejuízo para o CRCMG.

Art. 8º Todo processo administrativo de licitação será elaborado, instruído e acompanhado pela Gerência Administrativa e Financeira do CRCMG e submetido para análise e parecer da Assessoria Jurídica.

Parágrafo único. A análise e a aprovação das minutas dos atos convocatórios são de competência exclusiva da Assessoria Jurídica do CRCMG, nos termos do parágrafo único do artigo 38 da Lei n.º 8.666/1993.

Art. 9º Será franquiada vista dos autos de todos os processos administrativos de licitação para o Controlador Interno do CRCMG, que poderá auditá-los, emitir parecer de auditoria sobre a legalidade, economicidade e legitimidade dos procedimentos e determinar medidas corretivas quando verificadas inconsistências ou erros formais que não comprometam o interesse público da compra e não configurem restrição de mercado ou direcionamento, em qualquer fase da licitação.

Parágrafo único. Quando constatados, em auditoria, indícios de ilegalidade ou irregularidade em autos, estes deverão ser remetidos imediatamente à autoridade competente, acompanhados do parecer de auditoria, para a devida apreciação e, se confirmado o fato, deve ser realizada a publicação do ato de anulação.

Art. 10. Após encerrada a etapa de disputa, recursos e adjudicação, os autos processuais serão submetidos à apreciação do Presidente do CRCMG ou, em caso de indisponibilidade deste, do Vice-Presidente de Administração e Planejamento, que homologará o processo, desde que obedecidas as normas legais.

Parágrafo único. É facultada ao Presidente a remessa dos autos para a manifestação da Assessoria Jurídica antes da homologação dos processos administrativos de licitação, para manifestação quanto à conformidade com o rito processual.

Art. 11. Todos os funcionários designados por esta portaria estão sujeitos à avaliação periódica de conhecimentos técnicos, promovida pelo Controle Interno do CRCMG por processo sistemático de aferição do desempenho e conhecimento, a qual será utilizada para fins de programação de ações de capacitação e qualificação continuada.

Parágrafo único. A Gerência Administrativa e Financeira elaborará e coordenará a execução de programas de capacitação continuada de todos os membros da Comissão Permanente de Licitação e Pregoeiros.



Art. 12. Esta portaria entra em vigor a partir do dia 2 de setembro de 2022, ficando revogada a Portaria CRCMG n.º 125/2021.

Dê-se ciência aos interessados e cumpra-se.

Assinado digitalmente por:
SUELY MARIA MARQUES DE OLIVEIRA
CPF: 686.588.426-49
Certificado emitido por AC SOLUTI Multipla v5
Data: 24/08/2022 17:07:22 -03:00



Contadora Suely Maria Marques de Oliveira
Presidente



MANIFESTO DE ASSINATURAS



Código de validação: 4WMAB-36TVE-9DRTD-AVR6M

Esse documento foi assinado pelos seguintes signatários nas datas indicadas (Fuso horário de Brasília):

- ✓ SUELY MARIA MARQUES DE OLIVEIRA (CPF 686.588.426-49) em 24/08/2022 17:07 - Assinado com certificado digital ICP-Brasil

Para verificar as assinaturas, acesse o link direto de validação deste documento:

<https://assinador.crcmg.org.br/validate/4WMAB-36TVE-9DRTD-AVR6M>

Ou acesse a consulta de documentos assinados disponível no link abaixo e informe o código de validação:

<https://assinador.crcmg.org.br/validate>

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

MINUTA DE EDITAL

O **CONSELHO REGIONAL DE CONTABILIDADE DE MINAS GERAIS**, Autarquia Federal criada pelo Decreto-Lei nº 9.295/46, CNPJ: 17.188.574/0001-38, torna público, para ciência dos interessados, que por intermédio de seu Pregoeiro, designado pela Portaria CRCMG nº 117/2020, realizará licitação na modalidade **PREGÃO, na forma ELETRÔNICA**, do tipo **MENOR PREÇO**. O procedimento licitatório observará integralmente as disposições da Lei nº 10.520/2002, da Lei nº 13.709/2018, dos Decretos nº 3.555/2000, nº 7.746/2012, nº 8.538/2015, nº 9.178/2017, nº 9.507/2018 e nº 10.024/2019; da Lei Complementar nº 123/2006, alterada pelas Leis Complementares nº 155/2016 e nº 147/2014, das Instruções Normativas SEGES/MP nº 5/2017 e SEGES/MP nº 3/2018; aplicando-se, subsidiariamente, as normas da Lei nº 8.666/93, bem como pelas condições estabelecidas neste Edital.

DA SESSÃO PÚBLICA DO PREGÃO ELETRÔNICO:

A abertura da presente licitação dar-se-á em sessão pública, dirigida pelo Pregoeiro designado, a ser realizada de acordo com a legislação mencionada no preâmbulo deste Edital conforme indicado abaixo:

Data da abertura das propostas: **XX/XX/2023**

Horário da abertura das propostas: **XXhXXmin**, respeitando o horário de Brasília/DF.

Endereço eletrônico: www.comprasgovernamentais.gov.br

UASG: 925152

1. DO OBJETO

1.1. O objeto da presente licitação é a seleção da proposta mais vantajosa para a contratação de empresa especializada em **SERVIÇOS GERENCIADOS DE SEGURANÇA**, conforme condições e especificações estabelecidas no Anexo I – Termo de Referência deste Edital.

1.2. A licitação será realizada em único item.

1.3. O critério de julgamento adotado será o menor preço do item, observadas as exigências contidas neste Edital e seus Anexos quanto às especificações do objeto.

1.4. Integram este Edital os anexos I, II, III, IV, V, VI, VII e VIII.

2. DOS RECURSOS ORÇAMENTÁRIOS

2.1. As despesas para atender a esta licitação estão programadas em dotação orçamentária própria, prevista no plano de trabalho do CRCMG para o exercício de 2023, conforme indicação abaixo:

Projeto: 5002	Centro de Custo: 327	Conta contábil: 6.3.1.3.02.01.005

3. DO CREDENCIAMENTO

3.1. O Credenciamento é o nível básico do registro cadastral no SICAF, que permite a participação dos interessados na modalidade licitatória Pregão, em sua forma eletrônica.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

3.2. O cadastro no SICAF deverá ser feito no Portal de Compras do Governo Federal, no sítio www.comprasgovernamentais.gov.br, por meio de certificado digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP - Brasil.

3.3. O credenciamento junto ao provedor do sistema implica a responsabilidade do licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes a este Pregão.

3.4. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluindo a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

3.5. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais no SICAF e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

3.5.1. A não observância do disposto no subitem anterior poderá ensejar desclassificação no momento da habilitação.

4. DA PARTICIPAÇÃO NO PREGÃO

4.1. Poderão participar deste Pregão interessados cujo ramo de atividade seja compatível com o objeto desta licitação, e que estejam com Credenciamento regular no Sistema de Cadastramento Unificado de Fornecedores – SICAF, conforme disposto no art. 9º da IN SEGES/MP nº 3, de 2018.

4.1.1. Os licitantes deverão utilizar o certificado digital para acesso ao Sistema.

4.1.2. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no artigo 34 da Lei nº 11.488, de 2007, para o agricultor familiar, o produtor rural pessoa física e para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006.

4.2. Não poderão participar desta licitação os interessados:

4.2.1. proibidos de participar de licitações e celebrar contratos administrativos, na forma da legislação vigente;

4.2.2. que não atendam às condições deste Edital e seu(s) anexo(s);

4.2.3. estrangeiros que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;

4.2.4. que se enquadrem nas vedações previstas no artigo 9º da Lei nº 8.666, de 1993;

4.2.5. que estejam sob falência, recuperação judicial ou extrajudicial, ou concurso de credores ou insolvência, em processo de dissolução ou liquidação, observado o disposto no item 10.10.1.1 deste Edital;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

4.2.6. entidades empresariais que estejam reunidas em consórcio;

4.2.7. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição (Acórdão nº 746/2014-TCU-Plenário);

4.3. Nos termos do art. 5º do Decreto nº 9.507, de 2018, é vedada a contratação de pessoa jurídica na qual haja administrador ou sócio com poder de direção, familiar de:

4.3.1. detentor de cargo em comissão ou função de confiança que atue na área responsável pela demanda ou contratação;

4.3.2. Para os fins do disposto neste item, considera-se familiar o cônjuge, o companheiro ou o parente em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau (Súmula Vinculante/STF nº 13, art. 5º, inciso V, da Lei nº 12.813, de 16 de maio de 2013 e art. 2º, inciso III, do Decreto nº 7.203, de 04 de junho de 2010);

4.4. Nos termos do art. 7º do Decreto nº 7.203, de 2010, é vedada, ainda, a utilização, na execução dos serviços contratados, de empregado da futura Contratada que seja familiar de agente público ocupante de cargo em comissão ou função de confiança nesta Entidade contratante.

4.5. Como condição para participação no Pregão, o licitante assinalará “sim” ou “não” em campo próprio do sistema eletrônico, relativo às seguintes declarações:

4.5.1. que cumpre os requisitos estabelecidos no artigo 3º da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49.

4.5.1.1. nos itens exclusivos para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame;

4.5.1.2. nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte ou sociedade cooperativa.

4.5.2. que está ciente e concorda com as condições contidas no Edital e seus anexos;

4.5.3. que cumpre os requisitos para a habilitação definidos no Edital e que a proposta apresentada está em conformidade com as exigências editalícias;

4.5.4. que inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores;

4.5.5. que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7º, XXXIII, da Constituição;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

4.5.6. que não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

4.5.7. que os serviços são prestados por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação, conforme disposto no art. 93 da Lei nº 8.213, de 24 de julho de 1991.

4.6. A declaração falsa relativa ao cumprimento de qualquer condição sujeitará o licitante às sanções previstas em lei e neste Edital.

5. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

5.1. Os licitantes encaminharão, exclusivamente por meio do sistema, concomitantemente com os documentos de habilitação exigidos no edital, proposta com a descrição do objeto ofertado e o preço, até a data e o horário estabelecidos para abertura da sessão pública, quando, então, encerrar-se-á automaticamente a etapa de envio dessa documentação.

5.1.1. Os documentos de habilitação a que se refere o item acima são aqueles previstos no **ITEM 10 - DA HABILITAÇÃO** deste Edital.

5.1.2. Será desclassificado o licitante que não inserir no sistema previamente à abertura da sessão pública, a proposta de preços e os documentos de habilitação exigidos no **ITEM 10 - DA HABILITAÇÃO** ou que apresentá-los em desacordo com o estabelecido neste Edital.

5.2. O envio da proposta, acompanhada dos documentos de habilitação exigidos neste Edital, ocorrerá por meio de chave de acesso e senha.

5.3. Os licitantes poderão deixar de apresentar os documentos de habilitação que constem do SICAF, assegurado aos demais licitantes o direito de acesso aos dados constantes dos sistemas.

5.4. As Microempresas e Empresas de Pequeno Porte deverão encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art. 43, § 1º da LC nº 123, de 2006.

5.5. Incumbirá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

5.6. Até a abertura da sessão pública, os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema.

5.7. Não será estabelecida, nessa etapa do certame, ordem de classificação entre as propostas apresentadas, o que somente ocorrerá após a realização dos procedimentos de negociação e julgamento da proposta.

5.8. Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados para avaliação do pregoeiro e para acesso público após o encerramento do envio de lances.

6. DO PREENCHIMENTO DA PROPOSTA

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

6.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

6.1.1. **Valor unitário e total do item;**

6.1.2. Descrição do objeto, contendo as informações similares à especificação do Termo de Referência.

6.2. Todas as especificações do objeto contidas na proposta vinculam a Contratada.

6.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na prestação dos serviços;

6.3.1. A Contratada deverá arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do §1º do artigo 57 da Lei nº 8.666, de 1993.

6.3.2. Caso o eventual equívoco no dimensionamento dos quantitativos se revele superior às necessidades da contratante, a Administração deverá efetuar o pagamento seguindo estritamente as regras contratuais de faturamento dos serviços demandados e executados, concomitantemente com a realização, se necessário e cabível, de adequação contratual do quantitativo necessário, com base na alínea "b" do inciso I do art. 65 da Lei n. 8.666/93 e nos termos do art. 63, §2º da IN SEGES/MP n.5/2017.

6.4. O licitante é o único responsável pela cotação correta dos encargos tributários. Em caso de erro ou cotação incompatível com o regime tributário a que se submete, serão adotadas as orientações a seguir:

6.4.1. cotação de percentual menor que o adequado: o percentual será mantido durante toda a execução contratual;

6.4.2. cotação de percentual maior que o adequado: o excesso será suprimido, unilateralmente, da planilha e haverá glosa, quando do pagamento, e/ou redução, quando da repactuação, para fins de total ressarcimento do débito.

6.5. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses, devendo o licitante ou contratada apresentar ao pregoeiro ou à fiscalização, a qualquer tempo, comprovação da adequação dos recolhimentos, para os fins do previsto no subitem anterior.

6.6. Independentemente do percentual de tributo inserido na planilha, no pagamento dos serviços, serão retidos na fonte os percentuais estabelecidos na legislação vigente.

6.7. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar os serviços nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

6.8. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

6.9. O prazo de validade da proposta não será inferior a 60 (sessenta) dias, a contar da data de sua apresentação.

6.10. Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais, quando participarem de licitações públicas.

6.10.1. O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a responsabilização pelo Tribunal de Contas da União e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

7. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

7.1. A abertura da presente licitação dar-se-á em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

7.2. O Pregoeiro verificará as propostas apresentadas, desclassificando desde logo aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital, contenham vícios insanáveis ou não apresentem as especificações técnicas exigidas no Termo de Referência.

7.2.1. Também será desclassificada a proposta que identifique o licitante.

7.2.2. A desclassificação será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

7.2.3. A não desclassificação da proposta não impede o seu julgamento definitivo em sentido contrário, levado a efeito na fase de aceitação.

7.3. O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.

7.4. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

7.5. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio do sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

7.5.1. O lance deverá ser ofertado pelo **VALOR TOTAL DO ITEM**.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

7.6. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

7.7. O licitante somente poderá oferecer lance de valor inferior ou percentual de desconto superior ao último por ele ofertado e registrado pelo sistema.

7.8. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de 100,00 (cem reais).

7.9. Será adotado para o envio de lances no pregão eletrônico o **modo de disputa “aberto”**, em que os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

7.10. A etapa de lances da sessão pública terá duração de dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.

7.11. A prorrogação automática da etapa de lances, de que trata o item anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

7.12. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente.

7.13. Encerrada a fase competitiva sem que haja a prorrogação automática pelo sistema, poderá o pregoeiro, assessorado pela equipe de apoio, justificadamente, admitir o reinício da sessão pública de lances, em prol da consecução do melhor preço.

7.14. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

7.15. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

7.16. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

7.17. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.

7.18. O Critério de julgamento adotado será o **MENOR PREÇO**, conforme definido neste Edital e seus anexos.

7.19. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

7.20. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da LC nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

7.21. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da proposta ou lance de menor preço serão consideradas empatadas com a primeira colocada.

7.22. A melhor classificada nos termos do item anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

7.23. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

7.24. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

7.25. A ordem de apresentação pelos licitantes é utilizada como um dos critérios de classificação, de maneira que só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

7.25.1. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 3º, § 2º, da Lei nº 8.666, de 1993, assegurando-se a preferência, sucessivamente, aos serviços:

7.25.1.1. produzidos no país;

7.25.1.2. produzidos ou prestados por empresas brasileiras;

7.25.1.3. produzidos ou prestados por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

7.25.1.4. produzidos ou prestados por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação.

7.26. Persistindo o empate, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas empatadas.

7.27. Antes de seguir para a etapa de negociação, o pregoeiro irá certificar-se de que o licitante detentor da proposta vencedora enviou, por meio do sistema, os documentos de habilitação exigidos no edital e a proposta

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

de preços, nos termos do item 5 - DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO - deste Edital e, caso não tenha sido cumprida a exigência, a proposta será desclassificada.

7.28. Encerrada a etapa de envio de lances da sessão pública, o pregoeiro deverá encaminhar, pelo sistema eletrônico, contraproposta ao licitante que tenha apresentado o melhor preço, para que seja obtida melhor proposta, vedada a negociação em condições diferentes das previstas neste Edital.

7.28.1. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

7.29. Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

8. DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

8.1 O pregoeiro convocará o licitante melhor classificado para apresentar **no prazo de até 2 (duas) horas**, por meio do sistema eletrônico, **a proposta de preços final** ajustada à negociação realizada, acompanhada, se for o caso, de documentos complementares, quando necessários para confirmação de outro documento ou informação apresentados.

8.2. A proposta de preços final deverá:

8.2.1. ser redigida em língua portuguesa, datilografada ou digitada, em uma via, sem emendas, rasuras, entrelinhas ou ressalvas, devendo a última folha ser assinada e as demais rubricadas pelo licitante ou seu representante legal;

8.2.2. conter a identificação do licitante, os preços ofertados, em conformidade com último lance apresentado ou à negociação efetuada com o Pregoeiro, podendo utilizar como modelo o Anexo II deste Edital – Modelo de Proposta;

8.2.3. apresentar os preços ofertados, devidamente ajustados ao lance vencedor;

8.2.4. conter a indicação do banco, número da conta e agência do licitante vencedor, para fins de pagamento;

8.2.5. Somente mediante autorização do Pregoeiro e em caso de indisponibilidade do sistema, será aceito o envio da documentação por meio do e-mail licitacao@crcmg.org.br.

8.2.6. O prazo para envio da proposta poderá ser prorrogado, mediante solicitação escrita e justificada do licitante, via chat do sistema Comprasnet, formulada antes de findo o prazo estabelecido e formalmente aceita pelo Pregoeiro.

8.3. A proposta final deverá ser documentada nos autos e será levada em consideração no decorrer da execução do contrato e aplicação de eventual sanção à Contratada, se for o caso.

8.3.1. Todas as especificações do objeto contidas na proposta vinculam a Contratada.

8.4. Os preços deverão ser expressos em moeda corrente nacional, o valor unitário em algarismos e o valor global em algarismos e por extenso (art. 5º da Lei nº 8.666/93).

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

8.4.1. Ocorrendo divergência entre os preços unitários e o preço global, prevalecerão os primeiros; no caso de divergência entre os valores numéricos e os valores expressos por extenso, prevalecerão estes últimos.

8.5. A oferta deverá ser firme e precisa, limitada, rigorosamente, ao objeto deste Edital, sem conter alternativas de preço ou de qualquer outra condição que induza o julgamento a mais de um resultado, sob pena de desclassificação.

8.6. A proposta deverá obedecer aos termos deste Edital e seus Anexos, não sendo considerada aquela que não corresponda às especificações ali contidas ou que estabeleça vínculo à proposta de outro licitante.

8.7. As propostas que contenham a descrição do objeto, o valor e os documentos complementares estarão disponíveis na internet, após a homologação.

9. DA ACEITABILIDADE DA PROPOSTA VENCEDORA

9.1. Encerrada a etapa de negociação, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no parágrafo único do art. 7º e no § 9º do art. 26 do Decreto n.º 10.024/2019.

9.2. Será desclassificada a proposta ou o lance vencedor que apresentar preço final superior ao preço máximo fixado (Acórdão nº 1455/2018 - TCU - Plenário), ou que apresentar preço manifestamente inexequível.

9.2.1. Considera-se inexequível a proposta que apresente preços global ou unitários simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da licitação não tenha estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do próprio licitante, para os quais ele renuncie a parcela ou à totalidade da remuneração.

9.3. Qualquer interessado poderá requerer que se realizem diligências para aferir a exequibilidade e a legalidade das propostas, devendo apresentar as provas ou os indícios que fundamentam a suspeita;

9.3.1. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento das propostas, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, vinte e quatro horas de antecedência, e a ocorrência será registrada em ata;

9.4. O Pregoeiro poderá convocar o licitante para enviar documento digital complementar, por meio de funcionalidade disponível no sistema, **no prazo de 2 (duas) horas**, sob pena de não aceitação da proposta.

9.4.1. O prazo estabelecido poderá ser prorrogado pelo Pregoeiro por solicitação escrita e justificada do licitante, formulada antes de findo o prazo, e formalmente aceita pelo Pregoeiro.

9.4.2. Dentre os documentos passíveis de solicitação pelo Pregoeiro, destacam-se a Planilha de Custos e Formação de Preços, bem como os que contenham as características do material ofertado, tais como marca, modelo, tipo, fabricante e procedência, além de outras informações pertinentes, a exemplo de catálogos, folhetos ou propostas, encaminhados por meio eletrônico, ou, se for o caso, por outro meio e prazo indicados pelo Pregoeiro, sem prejuízo do seu ulterior envio pelo sistema eletrônico, sob pena de não aceitação da proposta.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

9.5. Será desclassificada a proposta ou o lance vencedor, nos termos do item 9.1 do Anexo VII-A da In SEGES/MP n. 5/2017, que:

9.5.1. não estiver em conformidade com os requisitos estabelecidos neste edital;

9.5.2. contenha vício insanável ou ilegalidade;

9.5.3. não apresente as especificações técnicas exigidas pelo Termo de Referência;

9.5.4. apresentar preço final superior ao preço máximo fixado (Acórdão nº 1455/2018 -TCU - Plenário), ou que apresentar preço manifestamente inexequível.

9.5.4.1. Quando o licitante não conseguir comprovar que possui ou possuirá recursos suficientes para executar a contento o objeto, será considerada inexequível a proposta de preços ou menor lance que:

9.5.4.1.1. for insuficiente para a cobertura dos custos da contratação, apresente preços global ou unitários simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da licitação não tenha estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do próprio licitante, para os quais ele renuncie a parcela ou à totalidade da remuneração.

9.5.4.1.2. apresentar um ou mais valores da planilha de custo que sejam inferiores àqueles fixados em instrumentos de caráter normativo obrigatório, tais como leis, medidas provisórias e convenções coletivas de trabalho vigentes.

9.6. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, na forma do § 3º do artigo 43 da Lei nº 8.666, de 1993 e a exemplo das enumeradas no item 9.4 do Anexo VII-A da IN SEGES/MP N. 5, de 2017, para que a empresa comprove a exequibilidade da proposta.

9.7. Quando o licitante apresentar preço final inferior a 30% (trinta por cento) da média dos preços ofertados para o mesmo item, e a inexequibilidade da proposta não for flagrante e evidente pela análise da planilha de custos, não sendo possível a sua imediata desclassificação, será obrigatória a realização de diligências para aferir a legalidade e exequibilidade da proposta.

9.8. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante do serviço ou da área especializada no objeto.

9.9. Se a proposta ou lance vencedor for desclassificado, o Pregoeiro examinará a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação.

9.10. Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a continuidade da mesma.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

9.11. Nos itens não exclusivos para a participação de microempresas e empresas de pequeno porte, sempre que a proposta não for aceita, e antes de o Pregoeiro passar à subsequente, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida, se for o caso.

9.12. Encerrada a análise quanto à aceitação da proposta, o pregoeiro verificará a habilitação do licitante, observado o disposto neste Edital

10. DA HABILITAÇÃO

10.1. Como condição prévia ao exame da documentação de habilitação do licitante detentor da proposta classificada em primeiro lugar, o Pregoeiro verificará o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

10.1.1. SICAF;

10.1.2. Consulta Consolidada de Pessoa Jurídica do Tribunal de Contas da União (<https://certidoes-apf.apps.tcu.gov.br/>);

10.1.3. Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS, mantido pela Controladoria-Geral da União (<https://portal.datransparencia.gov.br/sancoes/consulta?ordenarPor=nomeSancionado&direcao=asc>);

10.1.4. Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça. (www.cnj.jus.br/improbidade_adm/consultar_requerido.php);

10.1.5. Lista de Inidôneos, mantida pelo Tribunal de Contas da União – TCU (<https://contas.tcu.gov.br/ords/f?p=1660:3:0>).

10.1.6. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força do artigo 12 da Lei nº 8.429, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.

10.1.6.1. Caso conste na Consulta de Situação do Fornecedor a existência de Ocorrências Impeditivas Indiretas, o gestor diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

10.1.6.1.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.

10.1.6.1.2. O licitante será convocado para manifestação previamente à sua desclassificação.

10.1.7. Constatada a existência de sanção, o Pregoeiro reputará o licitante inabilitado, por falta de condição de participação.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

10.1.8. No caso de inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos arts. 44 e 45 da Lei Complementar nº 123/2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

10.2. Caso atendidas as condições de participação, a habilitação do licitante será verificada por meio do Sistema de Cadastro Unificado de Fornecedores – SICAF, nos documentos por ele abrangidos, em relação à habilitação jurídica, à regularidade fiscal, à qualificação econômica financeira e habilitação técnica, conforme o disposto na Instrução Normativa SEGES/MP nº 03, de 2018.

10.2.1. O interessado, para efeitos de habilitação prevista na Instrução Normativa SEGES/MP nº 03, de 2018 mediante utilização do sistema, deverá atender às condições exigidas no cadastramento no SICAF até o terceiro dia útil anterior à data prevista para recebimento das propostas.

10.2.2. É dever do licitante atualizar previamente as comprovações constantes do SICAF para que estejam vigentes na data da abertura da sessão pública, ou encaminhar, em conjunto com a apresentação da proposta, a respectiva documentação atualizada.

10.2.3. O descumprimento do subitem acima implicará a inabilitação do licitante, exceto se a consulta aos sítios eletrônicos oficiais emissores de certidões feita pelo Pregoeiro lograr êxito em encontrar a(s) certidão(ões) válida(s), conforme art. 43, §3º, do Decreto 10.024, de 2019.

10.3. Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Edital e já apresentados, o licitante será convocado a encaminhá-los, em formato digital, via sistema, **no prazo de 2 (duas) horas**, sob pena de inabilitação.

10.3.1. O prazo para envio da documentação, acima previsto, poderá ser prorrogado, mediante solicitação escrita e justificada do licitante, via chat do sistema Comprasnet, formulada antes de findo o prazo estabelecido e formalmente aceita pelo Pregoeiro.

10.3.2. Somente mediante autorização do Pregoeiro e em caso de indisponibilidade do sistema, será aceito o envio da documentação por meio do e-mail licitacao@crcmg.org.br.

10.4. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não digitais quando houver dúvida em relação à integridade do documento digital.

10.4.1. Na hipótese de serem solicitados pelo pregoeiro, os documentos serão remetidos em original, por qualquer processo de cópia reprográfica, autenticada por tabelião de notas, ou por servidor da Administração, desde que conferidos com o original, ou publicação em órgão da imprensa oficial, para análise, no prazo de 2 (dois) dias úteis, à Gerência Administrativa e Financeira, para o endereço, rua Cláudio Manoel, 639, bairro Savassi, Belo Horizonte-MG, CEP 30.140-105, em envelope fechado e rubricado no fecho, especificando o número do pregão e os dados da empresa.

10.5. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

10.6. Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se o licitante for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

10.6.1. Serão aceitos registros de CNPJ de licitante matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

10.7. Ressalvado o disposto no item 5.3, os licitantes deverão encaminhar, nos termos deste Edital, a documentação relacionada nos itens a seguir, para fins de habilitação.

10.8. Habilitação Jurídica

10.8.1. No caso de Microempreendedor Individual – MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio www.portaldoempreendedor.gov.br;

10.8.2. No caso de empresário individual, inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

10.8.3. No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;

10.8.4. Inscrição no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz, no caso de ser o participante sucursal, filial ou agência;

10.8.5. No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

10.8.6. Decreto de autorização, em se tratando de sociedade empresária estrangeira em funcionamento no País;

10.8.7. No caso de sociedade cooperativa: ata de fundação e estatuto social em vigor, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, bem como o registro de que trata o art. 107 da Lei nº 5.764, de 1971.

10.8.8. Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

10.9. Regularidade Fiscal e Trabalhista

10.9.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso.

10.9.2. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

10.9.3. Prova de regularidade perante o Fundo de Garantia por Tempo de Serviço – FGTS (Certificado de Regularidade do FGTS – CRF).

10.9.4. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de Certidão Negativa ou Positiva com Efeito de Negativa de Débitos Trabalhistas – CNDT, expedida pelo Tribunal Superior do Trabalho, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei 5.452, de 1º de maio de 1943.

10.9.5. Prova de inscrição no cadastro de contribuintes municipal, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

10.9.6. Prova de regularidade com a Fazenda Municipal do domicílio ou sede do licitante, relativa à atividade em cujo exercício contrata ou concorre;

10.9.7. Caso o licitante seja considerado isento dos tributos municipais relacionados ao objeto licitatório, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda Municipal do seu domicílio ou sede, ou outra equivalente, na forma da lei;

OU

10.9.5. Prova de inscrição no cadastro de contribuintes estadual, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

10.9.6. Prova de regularidade com a Fazenda Estadual do domicílio ou sede do licitante, relativa à atividade em cujo exercício contrata ou concorre;

10.9.7. Caso o licitante seja considerado isento dos tributos estaduais relacionados ao objeto licitatório, deverá comprovar tal condição mediante declaração da Fazenda Estadual do seu domicílio ou sede, ou outra equivalente, na forma da lei;

10.9.8. Caso o licitante detentor do menor preço seja qualificado como microempresa ou empresa de pequeno porte deverá apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição, sob pena de inabilitação.

10.10. Qualificação Econômico-Financeira

10.10.1. Certidão negativa de falência ou recuperação judicial, ou liquidação judicial, ou de execução patrimonial, conforme o caso, expedida pelo distribuidor da sede do licitante ou de seu domicílio, dentro do prazo de validade previsto na própria certidão, ou, na omissão desta, expedida há menos de 1 (um) ano contado da data da sua apresentação.

10.10.1.1. No caso de certidão positiva de recuperação judicial ou extrajudicial, o licitante deverá apresentar a comprovação de que o respectivo plano de recuperação foi acolhido judicialmente, na forma do art. 58, da Lei n.º 11.101, de 09 de fevereiro de 2005, sob pena de inabilitação, devendo, ainda, comprovar todos os demais requisitos de habilitação.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

10.10.1.2. Caso não conste no cadastro do SICAF do fornecedor a Certidão Negativa de Pedido de Falência e Concordata, o documento poderá ser consultado, pelo Pregoeiro, nos respectivos sítios oficiais emissores.

10.10.2. Balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta;

10.10.2.1. no caso de empresa constituída no exercício social vigente, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade;

10.10.2.2. é admissível o balanço intermediário, se decorrer de lei ou contrato/estatuto social.

10.10.3. comprovação da boa situação financeira da empresa mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), obtidos pela aplicação das seguintes fórmulas:

$$\begin{aligned}
 \text{LG} &= \frac{\text{Ativo Circulante} + \text{Realizável a Longo Prazo}}{\text{Passivo Circulante} + \text{Passivo Não Circulante}} \\
 \text{SG} &= \frac{\text{Ativo Total}}{\text{Passivo Circulante} + \text{Passivo Não Circulante}} \\
 \text{LC} &= \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}
 \end{aligned}$$

10.10.4. As empresas, cadastradas ou não no SICAF, que apresentarem resultado inferior ou igual a 1(um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverão comprovar patrimônio líquido de 10% (dez por cento) do valor estimado da contratação ou do item pertinente.

10.11. Qualificação técnica operacional e profissional

10.11.1. Qualificação técnica operacional

10.11.1.1. Como qualificação técnica, o licitante deverá apresentar juntamente com os documentos de habilitação, pelo menos 01 (um) atestado de capacidade técnica, expedido por pessoa jurídica de direito público ou privado, que comprove ter prestado serviços, pelo prazo mínimo de 12 (doze) meses, condizentes minimamente com os seguintes serviços solicitados neste termo de referência, sendo válida a apresentação de mais de um documento para a comprovação do quantitativo exigido, sendo os serviços de maior relevância:

10.11.1.1.1. Serviço de Gestão de Vulnerabilidades, por meio do fornecimento, instalação, prestação de serviços de suporte, administração e operação da solução para no mínimo, 150 (cento e cinquenta) ativos de TI. Este item visa atestar a capacidade da licitante para o fornecimento do serviço especificado no Item SERVIÇO DE GESTÃO VULNERABILIDADE exigido neste certame.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

10.11.1.1.2. Serviços Gerenciado de monitoramento, triagem, tratamento e resposta a incidentes de segurança, utilizando tecnologia de SIEM (Security Information and Event Management) para gerenciamento e correlação de eventos de segurança através da análise de Logs e pacotes, em redes com, no mínimo, 150 (centos e cinquenta) ativos de TI.

10.11.1.1.3. Disponibilidade de Centro de Operações de Segurança que disponha de dois tipos de conexões digitais com a CONTRATADA, a fim de garantir a redundância e disponibilidade das conexões do Centro de Operações de Segurança.

10.11.1.2. O atestado deverá ser apresentado em papel timbrado da pessoa jurídica, contendo a identificação do signatário, nome, endereço, telefone e, se for o caso, correio eletrônico, para contato, e deve indicar as características, quantidades e prazos das atividades executadas ou em execução pela licitante vencedora.

10.11.1.3. Os atestados de capacidade técnica apresentados poderão ser objeto de diligência a critério do CRCMG, para verificação da autenticidade de seu conteúdo. Encontrada qualquer divergência entre a informação apresentada pela licitante vencedora e o apurado em eventual diligência, inclusive validação do contrato de prestação de serviço assinado entre o emissor e a licitante, além da desclassificação sumária do Pleito, a empresa fica sujeita às penalidades cabíveis e aplicáveis.

10.11.1.4. Para a comprovação da experiência mínima de 12 (doze) meses, será aceito o somatório de atestados de períodos diferentes.

10.11.2. Qualificação técnica profissional

10.11.2.1. Declaração formal de disponibilidade técnica, em papel timbrado da licitante, atestando que terá disponível, em seu quadro de pessoal, quando da assinatura do contrato e o consequente início da prestação dos serviços, equipe de profissionais com as qualificações técnicas obrigatórias e necessárias à execução dos serviços, objeto deste Edital, devendo constar as informações como, cargo, certificações e descrições acerca dos conhecimentos e experiências, conforme modelo de declaração constante do Anexo VII - Declaração Formal de Disponibilidade Técnica - Qualificação Técnica dos Profissionais da Empresa.

10.11.2.1.1. As certificações e os conhecimentos e experiências dos profissionais deverão atender aos requisitos mínimos estabelecidos no Termo de Referência, conforme modelo de declaração constante do Anexo VII, para cada profissional, de acordo com sua área de atuação, sob pena de desclassificação da licitante.

10.11.2.1.2. No momento da assinatura do contrato, a empresa deverá comprovar o vínculo com os referidos profissionais, apresentando cópia da Carteira de Trabalho e Previdência Social (CTPS), no caso de haver relação de emprego, ou de contrato de prestação de serviços, regidos pela legislação civil.

10.11.2.1.3. Em todo caso, os profissionais deverão estar disponíveis à prestação dos serviços de modo permanente, durante toda a vigência contratual.

10.11.2.1.4. Não serão aceitos vínculos de natureza eventual ou precária, inclusive os decorrentes de terceirização ou subcontratação.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

10.11.3. Vistoria

10.11.3.1. **Atestado de vistoria** assinado pelo responsável técnico do CRCMG, conforme modelo constante do **Anexo V**, ou Declaração de ciência das informações e condições do local de execução dos serviços, conforme modelo constante do **Anexo VI**, assinada por representante da licitante, assumindo todos riscos e consequências relativos às condições dos locais de execução do objeto e peculiaridades inerentes à natureza do trabalho, podendo a licitante, escolher entre as duas opções, a que melhor estiver adequada para sua participação no certame.

10.11.3.2. Ressalta-se que **a vistoria não é obrigatória**. Contudo, caso o licitante não tenha interesse em realizá-la, deverá preencher e incluir no sistema eletrônico juntamente com os demais documentos de habilitação, a **Declaração de ciência das informações e condições do local de execução dos serviços**, conforme modelo constante do **Anexo VI**.

10.11.3.3. Caso o licitante opte por fazer a vistoria deverá agendá-la, com antecedência mínima de 3 (três) dias da data de abertura da sessão, através do e-mail licitacao@crcmg.org.br.

10.12. O licitante enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado (a) da prova de inscrição nos cadastros de contribuintes estadual e municipal e (b) da apresentação do balanço patrimonial e das demonstrações contábeis do último exercício.

10.13. A existência de restrição relativamente à regularidade fiscal e trabalhista não impede que a licitante qualificada como microempresa ou empresa de pequeno porte seja declarada vencedora, uma vez que atenda a todas as demais exigências do edital.

10.13.1. A declaração do vencedor acontecerá no momento imediatamente posterior à fase de habilitação.

10.14. Caso a proposta mais vantajosa seja ofertada por microempresa, empresa de pequeno porte ou sociedade cooperativa equiparada, e uma vez constatada a existência de alguma restrição no que tange à regularidade fiscal e trabalhista, a mesma será convocada para, no prazo de 5 (cinco) dias úteis, após a declaração do vencedor, comprovar a regularização. O prazo poderá ser prorrogado por igual período, a critério da administração pública, quando requerida pelo licitante, mediante apresentação de justificativa.

10.15. A não regularização fiscal e trabalhista no prazo previsto no subitem anterior acarretará a inabilitação do licitante, sem prejuízo das sanções previstas neste Edital, sendo facultada a convocação dos licitantes remanescentes, na ordem de classificação. Se, na ordem de classificação, seguir-se outra microempresa, empresa de pequeno porte ou sociedade cooperativa com alguma restrição na documentação fiscal e trabalhista, será concedido o mesmo prazo para regularização.

10.16. Havendo necessidade de analisar minuciosamente os documentos exigidos, o Pregoeiro suspenderá a sessão, informando no "chat" a nova data e horário para a continuidade da mesma.

10.17. Será inabilitado o licitante que não comprovar sua habilitação, seja por não apresentar quaisquer dos documentos exigidos, ou apresentá-los em desacordo com o estabelecido neste Edital.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

10.18. Nos itens não exclusivos a microempresas e empresas de pequeno porte, em havendo inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

10.18.1. O licitante provisoriamente vencedor em um item, que estiver concorrendo em outro item, ficará obrigado a comprovar os requisitos de habilitação cumulativamente, isto é, somando as exigências do item em que venceu às do item em que estiver concorrendo, e assim sucessivamente, sob pena de inabilitação, além da aplicação das sanções cabíveis.

10.18.1.1. Não havendo a comprovação cumulativa dos requisitos de habilitação, a inabilitação recairá sobre o(s) item(ns) de menor(es) valor(es), cuja retirada(s) seja(m) suficiente(s) para a habilitação do licitante nos remanescentes.

10.19. Constatado o atendimento às exigências de habilitação fixadas no Edital, o licitante será declarado vencedor.

11. DOS RECURSOS

11.1. O Pregoeiro declarará o vencedor e, depois de decorrida a fase de regularização fiscal e trabalhista de microempresa ou empresa de pequeno porte, se for o caso, concederá o prazo de, no mínimo, trinta minutos, para que qualquer licitante manifeste a intenção de recorrer, de forma motivada, isto é, indicando contra qual(is) decisão(ões) pretende recorrer e por quais motivos, em campo próprio do sistema.

11.2. Havendo quem se manifeste, caberá ao Pregoeiro verificar a tempestividade e a existência de motivação da intenção de recorrer, para decidir se admite ou não o recurso, fundamentadamente.

11.2.1. Nesse momento o Pregoeiro não adentrará no mérito recursal, mas apenas verificará as condições de admissibilidade do recurso.

11.2.2. A falta de manifestação motivada do licitante quanto à intenção de recorrer importará a decadência desse direito.

11.2.3. Uma vez admitido o recurso, o recorrente terá, a partir de então, o prazo de três dias para apresentar as razões, pelo sistema eletrônico, ficando os demais licitantes, desde logo, intimados para, querendo, apresentarem contrarrazões também pelo sistema eletrônico, em outros três dias, que começarão a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa de seus interesses.

11.2.4. Caso o licitante que manifestou intenção de recorrer não apresente o recurso fundamentado no sistema eletrônico dentro do prazo acima estabelecido, decaíra seu direito recursal e o pregoeiro dará prosseguimento à fase de adjudicação.

11.2.5. A Administração decidirá sob o recurso e enviará resposta no sistema eletrônico no prazo máximo de 10 (dez) dias contados do encerramento do prazo de contrarrazões.

11.3. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

11.4. Os autos do processo permanecerão com vista franqueada aos interessados, no endereço constante neste Edital.

12. DA REABERTURA DA SESSÃO PÚBLICA

12.1. A sessão pública poderá ser reaberta:

12.1.1. Nas hipóteses de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que dele dependam.

12.1.2. Quando houver erro na aceitação do preço melhor classificado ou quando o licitante declarado vencedor não assinar o contrato, não retirar o instrumento equivalente ou não comprovar a regularização fiscal, nos termos do art. 43, §1º da LC nº 123/2006. Nessas hipóteses, serão adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.

12.2. Todos os licitantes remanescentes deverão ser convocados para acompanhar a sessão reaberta.

12.2.1. A convocação se dará por meio do sistema eletrônico ("chat") ou e-mail, de acordo com a fase do procedimento licitatório.

12.2.2. A convocação feita por e-mail dar-se-á de acordo com os dados contidos no SICAF, sendo responsabilidade do licitante manter seus dados cadastrais atualizados.

13. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

13.1. O objeto da licitação será adjudicado à licitante declarada vencedora, por ato do Pregoeiro, caso não haja interposição de recurso, ou pela autoridade competente, após a regular decisão dos recursos apresentados.

13.2. Após a fase recursal, constatada a regularidade dos atos praticados, a autoridade competente homologará o procedimento licitatório.

14. DA GARANTIA DE EXECUÇÃO

14.1. Será exigida a prestação de garantia de execução, na presente contratação, conforme regras constantes do Contrato.

15. DO TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE

15.1. Após a homologação da licitação, em sendo realizada a contratação, será firmado Termo de Contrato ou emitido instrumento equivalente.

15.2. O adjudicatário terá o prazo de 5 (cinco) dias úteis, contados a partir da data de sua convocação, para assinar o Termo de Contrato ou aceitar instrumento equivalente, conforme o caso (Nota de Empenho/Carta Contrato/Autorização), sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

15.2.1. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do Termo de Contrato ou aceite do instrumento equivalente, a Administração poderá encaminhá-lo para assinatura ou aceite

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

da Adjudicatária, mediante correspondência postal com aviso de recebimento (AR) ou meio eletrônico, para que seja assinado e devolvido ou aceito no prazo de 5 (cinco) dias úteis, a contar da data de seu recebimento.

15.2.2. O prazo previsto no subitem anterior poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

15.3. O Aceite da Nota de Empenho ou do instrumento equivalente, emitida à empresa adjudicada, implica no reconhecimento de que:

15.3.1. referida Nota está substituindo o contrato, aplicando-se à relação de negócios ali estabelecida as disposições da Lei nº 8.666, de 1993;

15.3.2. a contratada se vincula à sua proposta e às previsões contidas no edital e seus anexos;

15.3.3. a contratada reconhece que as hipóteses de rescisão são aquelas previstas nos artigos 77 e 78 da Lei nº 8.666/93 e reconhece os direitos da Administração previstos nos artigos 79 e 80 da mesma Lei.

15.4. Previamente à contratação a Administração realizará consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018, e nos termos do art. 6º, III, da Lei nº 10.522, de 19 de julho de 2002, consulta prévia ao CADIN.

15.4.1. Nos casos em que houver necessidade de assinatura do instrumento de contrato, e o fornecedor não estiver inscrito no SICAF, este deverá proceder ao seu cadastramento, sem ônus, antes da contratação.

15.4.2. Na hipótese de irregularidade do registro no SICAF, o contratado deverá regularizar a sua situação perante o cadastro no prazo de até 05 (cinco) dias úteis, sob pena de aplicação das penalidades previstas no edital e anexos.

15.5. Na assinatura do contrato ou da ata de registro de preços, será exigida a comprovação das condições de habilitação consignadas no edital, que deverão ser mantidas pelo licitante durante a vigência do contrato ou da ata de registro de preços.

15.6. Na hipótese de o vencedor da licitação não comprovar as condições de habilitação consignadas no edital ou se recusar a assinar o contrato ou a ata de registro de preços, a Administração, sem prejuízo da aplicação das sanções das demais cominações legais cabíveis a esse licitante, poderá convocar outro licitante, respeitada a ordem de classificação, para, após a comprovação dos requisitos para habilitação, analisada a proposta e eventuais documentos complementares e, feita a negociação, assinar o contrato ou a ata de registro de preços.

15.7. As condições de entrega, de pagamento, vigência, reajuste, recebimento do objeto e fiscalização, obrigações da contratada e do contratante, sanções e rescisão obedecerão às disposições constantes do Termo de Referência – Anexo I deste Edital e da Lei nº 8.666/93.

16. DAS SANÇÕES ADMINISTRATIVAS.

16.1. Comete infração administrativa, nos termos da Lei nº 10.520/2002, o licitante/adjudicatária que:

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

16.1.1. Não assinar o termo de contrato ou aceitar/retirar o instrumento equivalente, quando convocada dentro do prazo de validade da proposta, salvo caso fortuito ou força maior;

16.1.2. Deixar de entregar a documentação exigida para o certame;

16.1.3. Apresentar documentação falsa exigida para o certame;

16.1.4. Não manter a proposta;

16.1.5. Cometer fraude fiscal; e

16.1.6. Comportar-se de modo inidôneo.

16.2. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

16.3. O licitante/adjudicatário que cometer qualquer das infrações discriminadas nos subitens anteriores, ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

16.3.1. Advertência por faltas leves, assim entendidas como aquelas que não acarretarem prejuízos significativos ao objeto da contratação

16.3.2. Multa de 10% (dez por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do licitante;

16.3.3. Suspensão temporária do direito de participar de licitação e impedimento de contratar com a Administração, pelo prazo de até 2 (dois) anos;

16.3.4. Impedimento de licitar e de contratar com órgãos e entidades da União e descredenciamento no SICAF, pelo prazo de até 5 (cinco) anos.

16.3.5. Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados;

16.4. A penalidade de multa pode ser aplicada cumulativamente com as demais sanções.

16.5. Se, durante o processo de aplicação de penalidade, houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

16.6. A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

16.7. Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

16.8. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente na Lei nº 9.784, de 1999.

16.9. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

16.10. As penalidades serão obrigatoriamente registradas no SICAF.

16.11. As sanções por atos praticados no decorrer da contratação estão previstas no Termo de Referência – Anexo I deste Edital.

17. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

17.1. Até 3 (três) dias úteis antes da data fixada para abertura da sessão pública, qualquer pessoa poderá impugnar este Edital.

17.2. A impugnação poderá ser realizada de forma eletrônica, pelo e-mail licitacao@crcmg.org.br ou por petição dirigida ou protocolada no endereço da sede do CRCMG, Rua Cláudio Manoel, 639, Savassi, Belo Horizonte – MG.

17.3. Caberá ao Pregoeiro, auxiliado pelos responsáveis pela elaboração deste Edital e seus anexos, decidir sobre a impugnação no prazo de até 2 (dois) dias úteis contados da data de recebimento da impugnação.

17.4. Acolhida a impugnação, será designada nova data para a realização do certame, exceto quando, inquestionavelmente, a alteração não afetar a formulação das propostas.

17.5. Os pedidos de esclarecimentos referentes a este processo licitatório deverão ser enviados ao Pregoeiro, até 3 (três) dias úteis anteriores à data fixada para abertura da sessão pública, por meio eletrônico, através do endereço www.comprasgovernamentais.gov.br ou pelo e-mail licitacao@crcmg.org.br.

17.6. O Pregoeiro responderá aos pedidos de esclarecimentos no prazo de 2 (dois) dias úteis, contado da data de recebimento do pedido, e poderá requisitar subsídios formais aos responsáveis pela elaboração do Edital e dos anexos.

17.7. As respostas aos pedidos de esclarecimentos serão divulgadas pelo sistema e vincularão os participantes e a Administração.

17.8. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.



Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

17.8.1. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo pregoeiro, nos autos do processo de licitação.

17.9. As respostas às impugnações e aos pedidos de esclarecimentos também serão disponibilizadas no sítio do CRCMG www.crcmg.org.br.

18. DAS DISPOSIÇÕES GERAIS

18.1. Da sessão pública do Pregão divulgar-se-á Ata no sistema eletrônico.

18.2. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo Pregoeiro.

18.3. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília – DF.

18.4. O licitante será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas e lances.

18.5. Incumbirá à licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

18.6. No julgamento das propostas e da habilitação, o Pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

18.7. A homologação do resultado desta licitação não implicará direito à contratação

18.8. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

18.9. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

18.10. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.

18.11. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

18.12. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.



Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

18.13. O Edital está disponibilizado, na íntegra, no endereço eletrônico www.crcmg.org.br, e também poderão ser lidos e/ou obtidos na sede do CRCMG no endereço Rua Cláudio Manoel, nº 639, Savassi, Belo Horizonte - MG, nos dias úteis, no horário das 9h às 17h, mesmo endereço e período no qual os autos do processo administrativo permanecerão com vista franqueada aos interessados.

18.14. O licitante é responsável pela fidelidade e legitimidade das informações prestadas e dos documentos apresentados em qualquer fase da licitação. A falsidade de qualquer documento apresentado ou a inverdade das informações nele contidas implicará a imediata desclassificação do licitante que o tiver apresentado, ou, caso tenha sido o vencedor, a rescisão do contrato, sem prejuízo das demais sanções cabíveis.

18.15. A comunicação entre o Pregoeiro e os licitantes será realizada, exclusivamente, por meio das ferramentas disponíveis no sistema Comprasnet, sendo vedado qualquer atendimento presencial ou por meio de ligações telefônicas.

18.16. É facultada ao Pregoeiro ou à autoridade superior do CRCMG, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou complementar a instrução do processo licitatório, vedada a inclusão posterior de documento ou informação que deveria constar no ato da sessão pública.

18.17. Após a abertura da sessão pública do pregão, não caberá desistência de proposta, salvo se por motivo justo decorrente de fato superveniente e aceito pelo Pregoeiro.

18.18. A presente licitação poderá ser anulada em qualquer tempo, desde que seja constatada irregularidade no processo e/ou em seu julgamento, ou revogada por conveniência do CRCMG, sem que caiba às licitantes qualquer indenização.

18.19. Os casos omissos serão resolvidos pelo Pregoeiro, nos termos da legislação pertinente e dos Princípios Gerais de Direito.

18.20. As dúvidas e divergências que, eventualmente, possam surgir e que não possam ser dirimidas diretamente entre as partes, ficarão sujeitas ao foro da Justiça Federal, Subseção de Belo Horizonte, renunciando-se a qualquer outro, por mais privilegiado que seja.

18.21. É de responsabilidade do licitante o acompanhamento do processo no sítio www.comprasgovernamentais.gov.br, até a data da realização da sessão pública, tendo em vista que quaisquer alterações referentes a este Edital serão disponibilizadas no referido endereço, opções Acesso Livre – Pregões – Agendados.

18.22. Integram este Edital, para todos os fins e efeitos, os seguintes anexos

- 18.22.1. Anexo I - Termo de Referência;
- 18.22.2. Anexo II - Modelo de Proposta;
- 18.22.3. Anexo III - Minuta do Contrato;
- 18.22.4. Anexo IV - Catálogo de Serviço;
- 18.22.4. Anexo V - Atestado de Vistoria;
- 18.22.5. Anexo VI - Declaração de Ciência das Informações e Condições de Execução dos Serviços;



Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

18.22.6. Anexo VII - Declaração formal de disponibilidade técnica - Qualificação técnica dos profissionais da empresa;

18.22.7. Anexo VIII - Modelo de Termo de Confidencialidade e Sigilo do Prestador.

Belo Horizonte, XX de XXXXX de 2023.

XXXXXXXXXXXXXXXXXXXXX
Presidente do CRCMG

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

ANEXO I - TERMO DE REFERÊNCIA

1. DO OBJETO

Contratação de empresa especializada em SERVIÇOS GERENCIADOS DE SEGURANÇA.

2. INDICAÇÃO DE RECURSOS ORÇAMENTÁRIOS

Centro de Custo: 327

Projeto: 5002

Conta contábil: 6.3.1.3.02.01.005

3. JUSTIFICATIVA DO INTERESSE PÚBLICO EVIDENCIADO

Considerando que nos últimos anos temos visto diversas instituições públicas e privadas sofrendo constantes ataques cibernéticos, e tendo em vista a implantação da LGPD no CRCMG, que exige a adoção de medidas de segurança mais eficazes, torna-se indispensável a aplicação de boas práticas de segurança da informação no ambiente tecnológico do CRCMG, a fim de torna-lo mais seguro e menos suscetível a esses ataques.

Diante do crescimento exponencial de ameaças e ataques sofridos a empresas privadas e órgãos públicos no Brasil e no mundo, investimentos contínuos em segurança da informação são fundamentais para a mitigação de riscos de segurança associados ao negócio de maneira a resguardar a confidencialidade, a disponibilidade e a integridade das informações.

O cenário de ameaças à segurança da informação não se resume somente em ataques aos serviços de TI pela Internet. Tentativas de acesso não autorizado, infecção por arquivos maliciosos (vírus), e-mails indesejados (SPAMs), engenharia social, entre outros, são exemplos de eventos que podem apresentar riscos à segurança de TI. Até mesmo colaboradores não conscientes ou mal-intencionados representam risco potencial à segurança da informação.

Na busca de aperfeiçoamento da sua missão institucional e gestão pública, o Conselho Regional de Contabilidade de Minas Gerais vem utilizando cada vez mais soluções de TI, disponibilizando aos seus colaboradores, profissionais contábeis e à sociedade diversos serviços relacionados à Tecnologia da Informação. Nesse cenário, diversas foram as mudanças: tanto em termos de quantidade de serviços oferecidos quanto em diversidade de soluções, o que contribui para o aumento dos riscos e da necessidade de monitoramento, à medida que cresce a oferta de serviços pela Internet.

Nesse sentido, incidentes de segurança da informação, como nas hipóteses de violação, roubo ou perda de informações custodiadas pelo CRCMG, podem constituir possíveis situações capazes de inviabilizar, senão a totalidade, parte das atividades desta Entidade. Assim, a ocorrência de eventuais sinistros poderia provocar o vazamento de informações e prejuízo à sua imagem, podendo ainda o Conselho ter que responder pelos danos causados.

Por esses motivos, e devido ao incidente ocorrido recentemente no ambiente, tendo em vista que o Conselho não dispõe de infraestrutura física e pessoal para o monitoramento e gerenciamento de dispositivos de segurança com diversos fornecedores (firewall, sistema de prevenção de intrusões de rede, gerenciamento unificado de ameaças), capazes de realizar ações contra incidentes de segurança de forma tempestiva e procedimental, torna-se necessária realizar a contratação de uma solução que forneça uma estrutura em segurança da informação adequada, de forma a propiciar a integridade, confidencialidade, autenticidade e a

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

disponibilidade dos dados, através de um monitoramento preventivo e contínuo de segurança da informação contra ataques cibernéticos e de serviço de resposta a incidentes de segurança.

A contratação pretendida está alinhada com o planejamento estratégico do CRCMG, uma vez que contribuirá para o alcance do objetivo da qualidade de “Assegurar meios e recursos que permitam o cumprimento das políticas e diretrizes da gestão”, bem como dos objetivos estratégicos de “garantir qualidade e confiabilidade nos processos e nos procedimentos” e “Assegurar adequada infraestrutura e suporte logístico às necessidades dos CRCs”.

4. AMBIENTE TECNOLÓGICO DA CONTRATANTE (HARDWARE E SOFTWARE)

Infraestrutura tecnológica:

- 1 Firewall + 1 centralizador de logs, registros e relatórios como serviço;
- 129 estações de trabalho;
- 7 servidores virtuais Windows;
- 4 servidores virtuais Linux
- 90 usuários de rede;
- 125 caixas de e-mail na GSuite;

5. ESCOPO DOS SERVIÇOS

5.1. Serviços de monitoramento de ataques cibernéticos e resposta a incidentes:

- 5.1.1. Visa o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados à CONTRATANTE, através de fornecimento de solução de correlacionamento de logs de aplicações, serviços e infraestrutura do CONTRATANTE, que possam gerar eventos de segurança da informação, aos quais devem ser analisados, remediados, contidos e documentados, podendo estes serem transformados em um incidente de segurança da informação, obedecendo um processo cíclico e rigoroso de gestão de eventos.

5.2. Serviços de Gestão de Vulnerabilidades:

- 5.2.1. Tem por objetivo, de forma proativa e recorrente, identificar possíveis vulnerabilidades de segurança da informação na infraestrutura, nas aplicações e nas contas de usuários do CONTRATANTE, a fim de evitar que ataques cibernéticos direcionados à CONTRATANTE obtenha sucesso, explorando tais vulnerabilidades já conhecidas.

5.3. Serviço de monitoramento, detecção e resposta a incidentes para Endpoints.

- 5.3.1. Visa a proteção, monitoramento contínuo e operação de solução dedicada a proteção de estações e servidores do CONTRATANTE, realizando de forma proativa o bloqueio de códigos maliciosos tipo vírus, Malware - blindando os ativos protegidos também contra Ransomware, oferecendo possibilidade de realização de “Rollback” de arquivos alvos de códigos maliciosos, oferecendo ainda suporte à investigação de ataques através da trilha de registros de eventos forense.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

6. REQUISITOS GERAIS DOS SERVIÇOS

6.1. Os requisitos gerais dos serviços definem os requisitos obrigatórios para todos os serviços que compõem o objeto SERVIÇOS GERENCIADOS DE SEGURANÇA.

6.1.1. A CONTRATADA deverá cumprir com os prazos de detalhamento e as informações com a periodicidade referenciada neste documento, segmentados pelas modalidades de prestação de serviço.

6.1.2. Todos os entregáveis mensais referenciados neste documento, a partir do terceiro mês de contrato, deverão ser exibidos comparando com os dois meses anteriores para comparação gráfica de evolução e desempenho.

6.2. São apresentadas, a seguir, as especificações técnicas mínimas dos serviços a serem ofertados referentes ao objeto. Os termos “possui”, “permite”, “suporta” e “é” implicam no fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo “ou” implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo “e” implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções.

6.3. A CONTRATADA deverá possuir ao menos 01 (um) Centro de operação de segurança, atendendo, no mínimo, as seguintes características:

6.4. CANAIS DE COMUNICAÇÃO

6.4.1. Para abertura de solicitações, a CONTRATADA deverá disponibilizar 03 (três) tipos de canais de comunicação, a saber:

Grupo de Tecnologia	Classificação
Linha telefônica	Tipo 1
E-mail com domínio registrado e de propriedade da CONTRATADA.	Tipo 2
Sistema de ITSM do inglês <i>Information Technology Service Management</i> (Gerenciamento de Serviços de TI).	Tipo 3

Tabela 1- Tipos de canais de comunicação

6.4.2. Independente do canal de comunicação utilizado pela CONTRATANTE, as solicitações devem ser convergidas, atualizadas, resolvidas e concentradas em um único sistema de ITSM (Gerenciamento de Serviços de TI). Ou seja, imaginando que a CONTRATANTE realize a abertura de uma nova solicitação de serviço via linha telefônica, no segundo que segue a sua solicitação, a mesma deve constar no sistema de ITSM, assim também deve se proceder com a utilização do canal de comunicação do tipo 2: via e-mail.

6.4.3. Sobre o canal de comunicação do tipo 1: via linha telefonia tais ligações obrigatoriamente devem ser atendidas e/ou recepcionadas por uma interface humana, não sendo permitida a utilização de URA (Unidade de Resposta Audível), e/ou qualquer uso de atendimento eletrônico.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 6.4.4. Para um eventual cenário de crise, ou seja, onde o negócio fim da CONTRATANTE estiver sendo fortemente afetado por um problema envolvendo a segurança da informação, a CONTRATADA deverá disponibilizar uma sala de videoconferência virtual de sua propriedade, onde a qualquer tempo poderá ser utilizada para reuniões emergenciais para tratamento de crises.
- 6.4.5. Tal sala deve estar disponível via internet e seu acesso deve obrigatoriamente ser criptografado, utilizando protocolo SSL do inglês Secure Socket Layer, com certificado digital emitido em nome da CONTRATADA. A CONTRATADA também deve garantir que os canais de comunicação utilizados pela sala de videoconferência utilizem protocolos para criptografia dos dados trafegados.
- 6.4.6. A sala virtual ainda deve ter capacidade para minimamente 10 (dez) pessoas da CONTRATANTE simultaneamente, e a fim de evitar eventuais perdas de tempo em momento de crise, a sala deve estar acessível a qualquer tempo, não sendo criada apenas no momento da crise.

6.5. HORÁRIO DE ATENDIMENTO

- 6.5.1. Os SERVIÇOS GERENCIADOS DE SEGURANÇA devem obrigatoriamente ser executados, ofertados e estar acessíveis à CONTRATANTE em regime de 24 (vinte quatro) horas por dia, 07 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, durante todo o período de vigência do contrato.
- 6.5.2. Todo o atendimento deve ser iniciado por profissionais da contratada que estejam em horário de trabalho no momento do atendimento. Não é permitido o uso de funcionários no chamado "Regime de Plantão", "Sobreaviso" e/ou sistemas similares onde o funcionário apenas passa a trabalhar no momento do incidente.
- 6.5.3. GESTÃO DE CATÁLOGO DE SERVIÇO DO AMBIENTE DE SEGURANÇA DA INFORMAÇÃO**
- 6.5.3.1. A fim de fornecer uma única fonte de informação sobre os SERVIÇOS GERENCIADOS DE SEGURANÇA, disponíveis para cada grupo de tecnologia dos itens de configuração do parque de segurança da informação da CONTRATANTE, será definido em conjunto com a CONTRATADA uma lista de serviços que a CONTRATADA deverá ser capaz de entregar. Tal definição deverá ser aceita por ambas as partes e ficar disponível para consulta.
- 6.5.3.2. É de responsabilidade da CONTRATADA manter, atualizar e revisar os serviços disponíveis para cada grupo de serviço. As responsabilidades da CONTRATANTE estão relacionadas a aprovação de um novo serviço, ou a aposentadoria de um ou mais serviços existentes.
- 6.5.3.3. O catálogo de serviço deverá ser mantido e administrado através do sistema de ITSM de responsabilidade da CONTRATADA, estando este disponível de forma online para a CONTRATANTE, onde essa poderá consultar, a qualquer tempo, os serviços disponíveis.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

6.5.3.4. Apesar de já existir uma definição prévia de parte dos serviços a serem entregues pela CONTRATADA, incluídas no presente termo de referência (**Anexo VII - CATÁLOGO DE SERVIÇO**), a CONTRATANTE, a qualquer tempo, poderá solicitar a inclusão de novos serviços, ou a retirada de um serviço, em comum acordo com a CONTRATADA.

6.5.3.5. Também se espera que tais revisões de continuidade de um serviço no catálogo de serviços seja sugerido por parte da CONTRATADA durante a execução do contrato. Todavia, não é de responsabilidade da CONTRATADA a retirada ou inclusão de um serviço, cabendo apenas à CONTRATANTE tal ação.

6.5.4. MODALIDADE DE ATENDIMENTO

6.5.4.1. A modalidade preferencial de atendimento será a do tipo remota, devendo ser realizada nas dependências da CONTRATADA caso necessário, obedecendo, obrigatoriamente, os critérios estabelecidos para sua execução, conforme previstos neste Termo de Referência.

6.5.4.2. Os atendimentos referentes ao objeto contratado, denominado SERVIÇOS GERENCIADOS DE SEGURANÇA, são ilimitados durante o período de vigência do contrato, ou seja, não existe limite para quantidade de horas, e/ou quantidade de atendimentos realizados, limitando-se apenas ao escopo.

6.5.5. ACESSIBILIDADE E CONFIDENCIALIDADE

6.5.5.1. Para garantir a qualidade e disponibilidade dos serviços remotos, entre a CONTRATANTE e o Centro de Operações de Segurança da CONTRATADA, deverá haver dois tipos de conexões digitais, a fim de garantir a redundância e disponibilidade das conexões do Centro de Operações de Segurança.

6.5.5.2. Ambas as conexões digitais devem ter velocidade de upload e download mínima de 10 (dez) Mbps, serem contratadas de operadoras e rotas distintas, e devem ser utilizadas única e exclusivamente para prestação dos serviços presentes no Termo de Referência.

6.5.5.3. Especificamente para o tipo de conexão digital internet, necessariamente precisará ter IP dedicado, e não serão aceitos contratos com linksxDSL (executada a tecnologia HDSL). Também, a fim de garantir a disponibilidade da conexão, deverá a CONTRATADA garantir que tal conexão esteja protegida contra-ataques de DDoS - do inglês Distributed Denial of Service.

6.5.5.4. É de responsabilidade da CONTRATADA a contratação e os custos relativos ao fornecimento dos links de internet junto às operadoras, durante todo o período de vigência do contrato.

6.5.5.5. A fim de garantir a segurança do tráfego bidirecional entre a CONTRATANTE e o Centro de Operações de Segurança da CONTRATADA, ambas as conexões devem ser criptografadas. Ou seja, a CONTRATADA deverá estabelecer duas VPN's - do Inglês Virtual Private

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

Network, do tipo Site To Site, para o Centro de Operações de Segurança.

6.5.5.6. A fim de garantir a segurança entre a CONTRATANTE e os Centro de Operações de Segurança da CONTRATADA, não será permitido Centro de Operações de Segurança terceirizado ou consórcio de CONTRATANTES. A CONTRATADA deve ter e manter Centro de Operações de Segurança próprio.

6.5.5.7. Por outro lado, a CONTRATADA deve revogar todas as credenciais relacionadas a soluções de sua responsabilidade, empregadas na prestação de serviços para a CONTRATANTE, bem como solicitar tais revogações à CONTRATANTE, para soluções de responsabilidade da CONTRATADA, no mesmo dia do encerramento das atividades.

6.5.5.8. Tais exigências visam proteger o CONTRATANTE contra o uso indevido de informações sob sua custódia, por parte de profissional da CONTRATADA, assim como estão em conformidade com boas práticas de gestão e governança de TI.

6.5.6. DO CENTRO DE OPERAÇÕES DE CIBERSEGURANÇA - CSOC (CYBER SECURITY OPERATION CENTER)

6.5.6.1. Os SERVIÇOS GERENCIADOS DE SEGURANÇA devem ser executados por meio de ao menos 01 (um) Centro de Operações de Segurança da CONTRATADA, devendo estar situado obrigatoriamente no Brasil.

6.6. O CSOC deve atender os requisitos mínimos, a saber:

- 6.6.1. Utilizar sistema de gerenciamento de CFTV, que viabilizem o rastreamento de pessoas dentro do ambiente da CONTRATADA e cujas imagens possam ser recuperadas;
- 6.6.2. Filmar toda a área, mantendo as imagens armazenadas por, no mínimo, 90 (noventa) dias;
- 6.6.3. Efetuar registro de entrada e saída dos visitantes, com identificação individual em todos os acessos ao CSOC;
- 6.6.4. Possuir solução de monitoramento de disponibilidade e desempenho.
- 6.6.5. O perímetro físico do CSOC deve ser equipado com sensor de intrusão e alarmes contra acesso indevido;
- 6.6.6. Ser vigiado de forma ininterrupta em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano;
- 6.6.7. Ter controle de acesso físico com pelo menos 2 (dois) dos seguintes fatores de autenticação, a saber: cartão de identificação magnético, biometria de leitura de digital, reconhecimento facial e análise de retina;
- 6.6.8. Funcionar em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

(trezentos e sessenta e cinco) dias por ano;

- 6.6.9. Possuir registro de entrada e saída de pessoas, mantido por, pelo menos, 90 dias.
- 6.6.10. Possuir sistemas redundantes de alimentação de energia.
- 6.6.11. Para o caso de CSOC que utilize datacenter próprio, possuir estrutura de armazenamento de dados que permita a manutenção dos registros dos eventos relacionados aos serviços contratados por, no mínimo, o prazo do contrato.
- 6.6.12. Ser configurado de forma que a falha de um dos equipamentos isoladamente NÃO interrompa a prestação dos serviços;
- 6.6.13. Ter sistema de provimento ininterrupto de energia elétrica, composto por grupo gerador e UPSs do inglês Uninterruptible Power Supply, para garantir a transição entre o fornecimento normal da energia e o grupo gerador;
- 6.6.14. Para o caso de CSOC que utilize datacenter próprio, ter componentes de segurança necessários para garantir a preservação dos dados em casos de incêndio e execução de plano de recuperação de catástrofes;
- 6.6.15. Deverá possuir processos implementados baseados na norma ABNT NBR ISO/IEC 27001.
- 6.7. Para o caso de CSOC que utilize datacenter próprio, as infraestruturas de datacenter devem estar situadas fora dos ambientes de CSOC, e devem obrigatoriamente atender aos requisitos técnicos elencados, a saber:**
- 6.7.1. Estrutura física dedicada e construída com a finalidade exclusiva de prestação de serviços de hospedagem de aplicações e equipamentos, de modo a garantir um ambiente seguro e controlado, ou seja, não poderá possuir instalações hidráulicas na infraestrutura do Data Center;
- 6.7.2. Todos os equipamentos envolvidos na solução a ser disponibilizada deverão possuir fontes redundantes;
- 6.7.3. Deverá possuir área de estacionamento livre e privado, com acesso seguro para desembarque e manuseio de equipamentos com vigilância armada;
- 6.7.4. Deverá possuir guarita com segurança armada em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano. A guarita de segurança deverá estar fora do prédio de Data Center, criando-se uma barreira física ao acesso do Data Center, ter acesso a todo o sistema de CFTV, inclusive em tempo real, e detecção de intrusos em todas as cercanias onde está localizado o Data Center;
- 6.7.5. Toda a área do Data Center deve ser desprovida de janelas, básculas ou quaisquer formas de acesso que não através dos controles de acesso;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 6.7.6. Garantir a disponibilidade de pessoas dedicadas, treinadas e responsáveis pela segurança de acesso ao prédio e aos equipamentos do ambiente em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano;
- 6.7.7. Utilizar câmeras digitais de circuito interno de televisão, monitoradas e gerenciadas cujas imagens possam ser posteriormente consultadas por um período mínimo de 90 (noventa) dias, viabilizando o rastreamento de pessoas dentro do ambiente;
- 6.7.8. As câmeras digitais de circuito interno de televisão deverão cobrir todos os ângulos do túnel frio de forma que não existam quaisquer pontos cegos. A gravação e visualização em tempo real deverá ser feita em alta-resolução e em cores, com no mínimo 10 frames por segundo. Tais características são necessárias para que seja possível identificação da face daqueles que pretendem adentrar as cercanias do prédio do Data Center;
- 6.7.9. Sistema de detecção e combate a incêndio com uso de sensores de fumaça e fogo distribuídos pela área do Data Center e uso de descarga de gás com efeito supressor de combustão ou redução de oxigênio, ecologicamente aceitável e que não afeta pessoas e equipamentos energizados;
- 6.7.10. Garantir a detecção precoce de gases no ambiente incluindo a área situada sob o piso elevado utilizando detector VESDA, com sistema integrado de alarme monitorado e acompanhado em regime 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano;
- 6.7.11. Possuir sistema integrado aos túneis de ventilação do Data Center, de forma que em havendo o disparo de gás, o fluxo de ar é interrompido para a área do evento garantindo a extinção do incêndio sem afetar demais áreas do Data Center;
- 6.7.12. Em caso de sinistro, o disparo do gás deve ocorrer de forma automática, não havendo necessidade de intervenção humana;
- 6.7.13. O sistema de detecção precoce e combate a incêndio deverá possuir contrato de manutenção contemplando visitas preventivas e testes do sistema com o fabricante do mesmo no mínimo a cada 03 (três) meses;
- 6.7.14. A solução de ar-condicionado deve ser integrada a solução de combate a incêndio para que, em caso de incêndio, os dutos de ventilação sejam automaticamente fechados sem necessidade de intervenção humana;
- 6.7.15. Os equipamentos utilizados para prestação de serviços da CONTRATANTE deverão estar instalados em racks que trabalhem dentro de um sistema de Túnel Frio;
- 6.7.16. A climatização deverá ser composta por, no mínimo, segurança N+1 de unidades evaporadoras e, no mínimo, segurança N+1 de condensadoras externas ao edifício, interligadas por tubos de cobre isolados adequadamente;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 6.7.17. A climatização não deverá fazer troca de ar atmosférico. Tanto a sala de servidores quanto a sala de refrigeração deverão ser fechadas para que variações de temperatura, umidade e outros contaminantes não afetem os equipamentos dentro do Data Center;
- 6.7.18. Estar equipada com subestação elétrica própria e projetada para operar em média ou alta tensão, para atendimento aos requisitos de potência e alimentação elétrica adequadas e exclusivos para o Data Center;
- 6.7.19. Os sistemas devem ser equipados e protegidos por Nobreaks, bancos de baterias e geradores que funcionam automaticamente no caso de queda do fornecimento comercial;
- 6.7.20. Cada Nobreak deve possuir capacidade suficiente em regime N+1 para suportar todas as atividades do Data Center, incluindo as atividades previstas por este termo de referência;
- 6.7.21. Os nobreaks que atendem aos circuitos redundantes devem operar em regime Standalone, de maneira que os Nobreaks sejam completamente independentes entre si e sem risco de que a falha do primeiro se propague para o segundo;
- 6.7.22. O Data Center deve possuir sistema de geração elétrica à diesel próprio e redundante, que mantenha o ambiente em pleno funcionamento, durante todo o período de eventual corte de energia pela concessionária;
- 6.7.23. A autonomia do sistema de geração elétrica a diesel (grupo gerador) deverá ser de no mínimo 48 (quarenta e oito) horas sem reabastecimento de combustível.
- 6.7.24. Os geradores devem ser capazes de ser acionados para proteger o Data Center automaticamente não apenas em eventos de falta de energia, mas também quando algum parâmetro da concessionária estiver fora das especificações (frequência, tensão etc.);
- 6.7.25. No retorno da alimentação da concessionária, os grupos geradores devem ser capazes de sincronizarem sua alimentação e fazer a retirada da carga em rampa para evitar oscilações elétricas dentro do Data Center;
- 6.7.26. Os geradores e Nobreaks devem possuir contrato de manutenção contemplando visitas preventivas e testes do sistema com o fabricante dos mesmos com periodicidade mínima 1(uma) vez por mês;
- 6.7.27. O prédio da CONTRATADA deve atender a norma NBR 5410 para proteção de surto em todas as zonas.
- 6.7.28. Deve ser um sistema autônomo (AS) em relação à Internet por cadastro próprio, ou seja, possuir seus próprios blocos de IPv4, IPv6 e seu registro individual de ASN.
- 6.7.29. deverá possuir Solução Anti-DDoS, implementando proteção contra-ataques coordenados provenientes de múltiplos sistemas (comprometidos) e distribuídos geograficamente com o

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

intuito de gerar indisponibilidade dos serviços da CONTRATANTE através do esgotamento dos recursos.

- 6.7.30. Deverá ser fornecido o hardware que suporte todas as soluções presentes no Termo de Referência.
- 6.7.31. Possuir ambiente dedicado único e exclusivo para laboratório, onde seja possível reproduzir os incidentes e problemas da CONTRATANTE, sem que haja impacto na operação do Centro de Operações de Segurança e/ou da própria CONTRATANTE;
- 6.7.32. Possuir no Centro de Operações de Segurança processos consistentes e objetivos de monitoramento e detecção de ameaças, gestão de dispositivos, gestão de incidentes, inteligência de ameaças, investigação de ameaças e gestão de conformidade de segurança.
- 6.7.33. Possuir nativamente solução de SecOps para gerenciamento de incidentes de segurança da informação.
- 6.7.34. Deverá possuir processos implementados que garantam o cumprimento das normas e Lei Geral de Proteção de Dados. Tal exigência visa garantir controles rígidos e auditáveis de acesso físico e lógico às informações e monitoramento, além de comprovadamente contar com um comitê responsável pelos controles e adequações;

7. CONDIÇÕES GERAIS PARA PRESTAÇÃO DOS SERVIÇOS

- 7.1. Independentemente do grupo de serviço especificado, todas as soluções e/ou ferramentas utilizadas para prestação do serviço deverão obrigatoriamente seguir os requisitos, a saber:
 - 7.1.1. Deverá ser obrigatoriamente de propriedade da CONTRATADA ou licenciada para a CONTRATADA, não podendo ser do tipo *Open Source* (software livre).
 - 7.1.2. Deverá ser prestado por meio de solução provida através da nuvem do fabricante ou da CONTRATADA.
 - 7.1.3. Deve englobar o fornecimento de *Hardwares* e de *Softwares* necessários à execução dos serviços contratados durante o prazo de vigência do contrato, incluindo garantia, manutenção, atualização dos produtos e monitoramento de segurança em regime de 24 (vinte quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano;
 - 7.1.4. Os softwares ofertados devem ser instalados e atualizados em sua versão mais estável e estar cobertos por contratos de suporte e atualização de versão do fabricante durante a vigência do respectivo item de serviço. Da mesma maneira, os equipamentos fornecidos para a prestação dos serviços devem estar cobertos por contratos de garantia do fabricante;
 - 7.1.5. O conjunto de requisitos especificados para cada serviço pode ser atendido por meio de composição com outros equipamentos ou softwares utilizados no atendimento aos demais itens, de maneira integrada, desde que não implique alteração da topologia de rede ou na

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

exposição de ativos a riscos de segurança da informação, em termos de integridade, confidencialidade ou disponibilidade.

7.2. EQUIPE DE INTELIGENCIA DE AMEAÇAS

- 7.2.1. A contratada deverá contar com uma equipe de inteligência de ameaças dedicada a identificar as intenções, capacidades e, prioritariamente, as oportunidades usadas pelos criminosos através da coleta, normalização, correlação e análise de dados, transformando-os em inteligência e entregando ao CONTRATANTE relatórios periódicos, apresentando dados de mercado e o atual cenário do ambiente do CLIENTE.
- 7.2.2. Esses dados poderão ser utilizados para melhora na proteção, seja na atuação direta com a equipe de *Hunting* em novos casos de uso ou mantendo o time da CONTRATANTE informados, através de Boletins de Ameaças.
- 7.2.3. A CONTRATADA deverá possuir célula que entregue informações através de fontes de inteligências abertas e/ou próprias, compartilhando informações de inteligência através do MISP (*Malware Information Sharing Platform*), executando também a gestão dele através da equipe local, bem gerindo a integração entre o MISP da CONTRATANTE como da CONTRATADA.
- 7.2.4. A plataforma deverá ter capacidade de identificar vulnerabilidades em, no máximo, um dia após o surgimento desta, executar o correlacionamento com o inventário informado pela CONTRATANTE e informar via evento no MISP sobre os sistemas vulneráveis.
- 7.2.5. A CONTRATADA deverá possuir plataforma de inteligência que informe IoCs (Indicadores de Comprometimento) contendo, no mínimo, *Hashes* de binários maliciosos nos formatos MD5, SHA1, SHA256, *Filename*, domínios maliciosos, URLs maliciosas, bem como IPs maliciosos com geolocalização e pontuação de risco, reduzindo a possibilidade de falso positivo;
- 7.2.6. Deve possuir equipe de *Threat Intelligence* que execute Análise de Superfície, um trabalho que avalia o ambiente na perspectiva de um agente malicioso em busca de eventuais brechas utilizando o *Framework* OSINT (Inteligência de Fontes Abertas) com foco na identificação de superfície de ataque e as possíveis oportunidades na perspectiva de um agente malicioso.
- 7.2.7. Deve executar de forma recorrente a Análise de Superfície, no mínimo trimestralmente, utilizando especialistas de *Cyber Threat Intelligence* na execução de um *Assessment* interno e análise externa utilizando técnicas de OSINT, apresentando informações dos perímetros com objetivo de entregar relatório, apontando de forma prática como tratar cada ponto identificado e apresentar um *Score* qualitativo de maturidade para a CONTRATANTE.

7.3. PORTAL DE INDICADORES DE SERVIÇO

- 7.3.1. O portal de indicadores deverá ser disponibilizado à CONTRATANTE e contemplar, no mínimo, os requisitos abaixo:

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 7.3.2. A CONTRATADA deverá disponibilizar um sistema em modelo SaaS (do inglês *Software As Service*), denominado portal de indicadores, para consolidação dos dados gerados pelas soluções que compõem o objeto.
- 7.3.3. O portal deverá estar acessível à CONTRATADA via *Internet*, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, e 365 (trezentos e sessenta e cinco) dias por ano, de maneira segura utilizando protocolo de criptografia SSL.
- 7.3.4. A CONTRATANTE terá direito a criação de usuários ilimitados com a função de criação de perfis para cada usuário, disponibilizando assim visões diferentes para cada nível de acesso.
- 7.3.5. Deverá disponibilizar para os usuários da CONTRATANTE a função de mudança de visão gráfica a critério de cada usuário. Isso quer dizer que apesar de um gráfico estar disposto em modelo de barras, caso o usuário identifique uma melhor visualização do modelo gráfico em forma de pizza, o sistema deve oferecer tal funcionalidade ou opção.
- 7.3.6. O portal ainda deverá disponibilizar os seguintes modelos gráficos para os usuários:
- a) Gráfico do tipo Pizza;
 - b) Gráfico do tipo Barra;
 - c) Gráfico do tipo linha;
 - d) Gráfico do tipo área;
 - e) Gráfico do tipo funil;
 - f) Gráfico do tipo bolha.
- 7.3.7. INDICADORES DE RISCO – KRI:**
- 7.3.7.1. Deverá ser exibido no portal a quantidade de Vulnerabilidades que estavam presentes na última auditoria realizada através de gráfico(s) com separação dos tipos/quantidades com a opção de “Drill Down”, possibilitando assim visualização de forma mais detalhada das vulnerabilidades listadas;
- 7.3.7.2. O portal deverá possuir recurso para filtrar apenas as vulnerabilidades relevantes, excluindo as de severidade média e/ou baixa.
- 7.3.8. INDICADORES DE META E PERFORMANCE – KGI e KPI:**
- 7.3.8.1. O portal de indicadores deverá possuir relatório gráfico indicando tempo médio dos atendimentos dos incidentes por fase de Análise, contenção, erradicação e recuperação, possibilitando a filtragem por período:
- 7.3.8.2. Últimos 15 dias;
 - 7.3.8.3. Últimos 30 dias;
 - 7.3.8.4. Últimos 45 dias.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

7.3.9. Deverá possuir gráfico comparativo entre os primeiros e últimos 15 incidentes analisados dentro de período filtrado, mostrando numa linha de tempo qual foi o incidente com o tempo de atendimento menor, maior e o tempo médio.

7.3.10. Deverá ser possível a consulta deste gráfico para cada uma das fases de atendimento (análise, contenção, erradicação e recuperação).

7.4. INDICADORES POR CATEGORIA MITRE ATT&CK:

7.4.1. O Portal de indicadores deverá possuir gráfico que separe e classifique os incidentes de acordo com as categorias existentes na base de conhecimento do MITRE ATT&CK, sendo elas no mínimo:

- a) Initial Access;
- b) Execution;
- c) Persistence;
- d) Privilege Escalation;
- e) Defense Evasion;
- f) Lateral Movement;
- g) Collection;
- h) Command and Control;
- i) Exfiltration;
- j) Impact.

7.4.2. Todos os indicadores exibidos pelo portal, devem possuir a funcionalidade *Drill Down*, para que os usuários possam criar visualizações e filtros dos dados exibidos.

7.4.3. Todos os indicadores exibidos pelo portal devem ainda possuir funcionalidade de exibição dos dados gerados do gráfico de maneira tabular, a fim de que seja possível aferir os dados brutos.

7.4.4. O portal deve armazenar os dados durante o período mínimo de 1 (um) ano e deverá permitir a criação de filtros por períodos.

7.4.5. A qualquer tempo a CONTRATANTE poderá solicitar os dados brutos coletados das soluções que compõem o objeto contratado.

7.4.6. Os dados exibidos pelo portal devem representar o ambiente em tempo de execução e de forma automática (*Real Time*).

7.4.7. O portal deverá possibilitar customizar limiares dos serviços e eventos para gerar alarmes de acordo com o acordo de nível de serviço definido no presente termo de referência;

7.4.8. Deverá prover mecanismo para análise de risco e métricas de disponibilidade através de relatórios e *Dashboards* de todas as soluções que compõem o objeto.

7.5. SERVIÇO DE ACOMPANHAMENTO DE ENTREGAS

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 7.5.1. Deverá ser provido um serviço de acompanhamento de entregas através de reuniões de preferência virtuais para cadência do contrato de forma quinzenal.
- 7.5.2. **Entregável:** Ata de reunião
- 7.5.3. Deverá ser feito o acompanhamento periódico dos indicadores listados no contrato para antecipar desvios e corrigi-los antes que saiam das conformidades exigidas;
- 7.5.4. **Entregável:** Acompanhamento periódico a partir das ferramentas de registro de chamado ou medição (Portal de Indicadores);
- 7.5.5. **Entregável:** Checklist periódico dos entregáveis do projeto, conforme RFP, TR, proposta técnica e afins.
- 7.5.6. Deverá ser feito o acompanhamento do cronograma de faturamento mensal do contrato;
- 7.5.7. Deverá manter a matriz de comunicação atualizada dos dois lados do contrato – quem a CONTRATADA deve acionar e quem a CONTRATANTE deve acionar em casos específicos ou de escalção.
- 7.5.8. **Entregável:** Documento formal conforme formato pré-estabelecido.

7.6. SERVIÇO DE CONFORMIDADE DE DESEMPENHO CONTRATUAL

- 7.6.1. Deve ser provido serviço de conformidade de desempenho do contrato no qual deverão ser providas reuniões mensais entre a CONTRATANTE e a CONTRATADA com intuito de validação da satisfação referente aos serviços prestados.
- 7.6.2. Estas reuniões devem servir para identificação das necessidades da CONTRATANTE onde deverão ser apontados problemas recorrentes ou pontuais que estejam impactando a qualidade da execução do contrato.
- 7.6.3. Após essas reuniões deverão ser formulados planos de ações corretivos para cada área/serviço que não esteja cumprindo os padrões de qualidade exigidos no contrato.
- 7.6.4. O serviço deve ser executado por um especialista em resolução de crises ou temas críticos da CONTRATADA que funcione como moderador entre o time de entrega da CONTRATADA com os gestores do contrato da CONTRATANTE.
- 7.6.5. Entende-se como CRISE a atuação que é ou será baseada no desenvolvimento de um plano de ação para temas que gerem ônus imediato à CONTRATANTE, ônus direto e imediato à CONTRATADA, risco de exposição do ambiente da CONTRATANTE, risco de cancelamentos de contratos. Além disso, crises serão tratadas em conjunto com todas as áreas envolvidas, até a finalização do plano de ação de correção.
- 7.6.6. O especialista responsável por este serviço deve atuar também na escalção de temas não

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

críticos do dia a dia do contrato que não estejam sendo respondidos devidamente pela CONTRATADA.

7.6.7. Entende-se como **ESCALAÇÃO** problemas diários da CONTRATANTE em que a tratativa não foi eficaz e efetiva e/ou fora do tempo esperado/acordado, fazendo com que a CONTRATANTE eleve o tema para um nível hierárquico superior da CONTRATADA. Exemplos:

7.6.7.1. Falta de atuação de algum time específico;

7.6.7.2. Falta de resposta à um e-mail, chamado e/ou questionamentos do CONTRATANTE;

7.6.7.3. Falta de solução à um problema sinalizado pelo CONTRATANTE;

7.6.7.4. Chamado em aberto, não atendido dentro do SLA acordado em contrato;

7.6.7.5. Insatisfação da CONTRATANTE sobre um entregável como relatório, boletins, atuação/postura de recursos ou times;

7.6.8. Este serviço deverá prover ainda um indicador denominado NPS (Net Promoter Score) que consiga metrificar a satisfação da CONTRATANTE em relação aos serviços prestados que estejam estipulados no contrato. Esta métrica deverá seguir os padrões e fórmulas comuns de mercado e deverá ser atualizada e apresentada mensalmente aos gestores do contrato.

7.6.9. Em quaisquer mudanças em que a CONTRATADA identifique possíveis impactos no ambiente, e/ou que necessite de alterações de configurações em servidores ou ferramentas que possuam amplo alcance deverão passar pelo processo de aprovação de RDM (Requisição de Mudança) da CONTRATANTE.

8. ESPECIFICAÇÃO DOS SERVIÇOS

8.1. SERVIÇOS DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS E RESPOSTA A INCIDENTES

8.1.1. Visa o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados a CONTRATANTE, através de fornecimento de serviços com capacidade de correlacionamento de eventos, para detecção de ameaças direcionadas a CONTRATADA para detecção de comportamento anômalo de serviços, que possam gerar eventos de segurança da informação, aos quais devem ser analisados, podendo estes serem transformados em um incidente de segurança da informação, obedecendo um processo cíclico e rigoroso de gestão de eventos.

8.1.2. SOBRE AS FERRAMENTAS A SEREM UTILIZADAS

8.1.2.1. Para execução deste serviço, a CONTRATADA deverá utilizar e ser capaz de fornecer, operar, sustentar e suportar soluções de monitoramento que atendam o descritivo técnico a seguir:

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 8.1.2.2. A plataforma utilizada deverá ter capacidade de operar com volumes massivos de dados em tempo real utilizando algoritmos de aprendizagem de automático de máquina “*Machine Learning*” e deve contar com casos de uso para detectar ameaças avançadas.
- 8.1.2.3. A plataforma deverá possuir as características a seguir:
- 8.1.2.4. Extremamente escalável e tolerante a falhas, capaz de ingerir centenas de terabytes por dia e suportar a retenção de eventos de segurança por longo período.
- 8.1.2.5. Junte-se a eventos ao longo do tempo usando modelos Kill Chain para a análise de eventos de maior risco.
- 8.1.2.6. Permitir o hunting rápido de ameaças por meio da pesquisa em linguagem natural.
- 8.1.2.6.1. A solução deve estar classificada como líder no quadrante mágico de “Security Information and Event Management” pelo menos no último ou penúltimo ano;
- 8.1.2.6.2. A solução deve ter recursos de “Multi-tenant”;
- 8.1.2.6.3. Deve ser do tipo Nuvem em Software como um modo de Serviço e ter as certificações SOC 2 TYPE II e ISO 27001.
- 8.1.2.6.4. Deve garantir retenção dos logs conforme arquitetura abaixo:
- a) 7 dias hot retention;
 - b) 90 dias warm retention;
 - c) 365 dias cold retention.
- 8.1.2.6.5. Deve ter alta disponibilidade e mecanismos de recuperação de desastres;
- 8.1.2.6.6. Deve permitir a filtragem e compressão de dados seletivos em até 90% no ponto de coleta;
- 8.1.2.6.7. Deve permitir o gerenciamento da largura de banda para a transmissão de dados entre os coletores e os servidores de gerenciamento;
- 8.1.2.6.8. Deve executar o armazenamento em cache local e/ou em buffer nos coletores para garantir que nenhum dado seja perdido em trânsito no caso de um problema de rede ou um pico no volume do evento;
- 8.1.2.6.9. Deve oferecer suporte ao mascaramento de dados por meio de controles de acesso granulares baseados em funções, para ofuscar qualquer informação de usuário potencialmente sensível na camada de interface do usuário;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 8.1.2.6.10. Deve suportar controle de acesso baseado em função granular (RBAC) com suporte a administração delegada, tanto para as funcionalidades na interface do usuário quanto acesso aos dados e configurações;
- 8.1.2.6.11. Deve incluir uma ferramenta de Security Datalake baseada em bigdata em uma arquitetura aberta e escalável e com capacidade de coletar e reter dados por períodos estabelecidos para fins de conformidade e investigação;
- 8.1.2.6.12. Deve ter uma instância de homologação para testes que permita isolar, do ambiente de produção, novas integrações, novos desenvolvimentos de conteúdos e novos analisadores;
- 8.1.2.6.13. A solução deve atender as seguintes características:
- 8.1.2.6.13.1. Deve oferecer suporte a integração com mais de 500 fontes de eventos usando métodos de syslog, formatos de log estruturados (CEF, LEEF, MEF, JSON, XML), arquivos, bancos de dados (conexão JDBC), conexão API (AWS, Azure, Box, Crowdstrike, Google Report, Netskope, SVN, Salesforce, Splunk, QRadar, Netwitness, Office 365, Okta, Proofpoint, Sumologic, Workday, entre outros), WMI, consultas LDAP/LDAPS, dados e fluxo (Netflow, sFlow, jFlow), Hadoop, Registros não estruturados (Regex), agentes de terceiros (snare);
- 8.1.2.6.14. Deve permitir a integração com diferentes tipos de fontes de dados, como dados de identidade, logs de atividades / transações, logs de eventos de segurança, fluxos de rede, log de aplicativos / plataformas de nuvem, permissões de acesso, fontes de inteligência de ameaças, dados não estruturados e metadados de ativos;
- 8.1.2.6.15. Deve permitir conexão a sistemas externos de gerenciamento de identidade, como Active Directory / LDAP ou soluções de IAM (gestão de identidade), como Aveksa/Sailpoint, sistemas de RH, como Peoplesoft/Workday, para realizar o enriquecimento contextual de eventos adicionando identidade do usuário;
- 8.1.2.6.16. Deve ser capaz de se conectar nativamente através de APIs ou outros meios com serviços em nuvem como Salesforce, Amazon Web Services S3 e Cloudtrail, BOX, Microsoft Azure, Office 365, Google Apps, Google Cloud, Netskop, ServiceNow, entre outros.
- 8.1.2.6.17. Deve ter uma interface de usuário que permita modificar conectores, analisadores (parsers) existentes ou construir novos analisadores (parsers) na mesma interface de usuário;
- 8.1.2.6.18. Deve ter conectores, analisadores (parsers) pré-configurados, prontos para uso, mas que possam ser modificados conforme necessário. A análise, normalização e categorização dos coletores devem ser totalmente personalizáveis na interface

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

do usuário.

- 8.1.2.6.19. Deve ter uma API RESTful de serviços para integração bidirecional com outras tecnologias;
- 8.1.2.6.20. Deve fornecer integração com pelo menos 5 fontes de inteligência de ameaças incluídas no valor do serviço ofertado;
- 8.1.2.6.21. Deve realizar o enriquecimento dos eventos com dados contextuais sobre eventos no momento da captura e ingestão de dados adicionando aos eventos:
 - a) Identidade do usuário;
 - b) Contexto de negócios;
 - c) Metadados de ativos;
 - d) Informações de rede;
 - e) Localização Geográfica;
 - f) Dados de inteligência de ameaças;
- 8.1.2.6.22. Deve enriquecer eventos em tempo real com contexto de usuário e entidade. Os dados ricos podem fornecer atributos de contexto que podem ser usados para perfis comportamentais, comparações de pares, pesquisas e investigações;
- 8.1.2.6.23. Deve detectar ameaças cibernéticas e internas avançadas (insider threat) usando aprendizado de máquina para criar perfis e linhas de base de comportamento de usuários e entidades;
- 8.1.2.6.24. Deve ter conteúdo pré-empacotado de casos de uso e modelos de ameaças prontos para uso para detecção avançada de ameaças, como:
 - a) Detecção de ameaças internas (insider threat) utilizando técnicas de aprendizagem de máquina;
 - b) Detecção de ameaças cibernéticas (cyber threat) utilizando técnicas de aprendizagem de máquina;
 - c) Detecção de ameaças na nuvem (cloud threat) utilizando técnicas de aprendizagem de máquina;
- 8.1.2.6.25. Deve fornecer recursos abrangentes para modelar e ajustar a pontuação de risco com base no perfil do usuário e/ou entidade, gravidade da ameaça e sequência/combinção de eventos que ocorrem durante um período;
- 8.1.2.6.26. Deve permitir a modelagem de risco a partir da interface do usuário de acordo com as prioridades da organização;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 8.1.2.6.27. Deve ter modelos de ameaças que permitam agrupar eventos realizados por um usuário ou entidade que duram dias, semanas, meses e assim por diante. Essas atividades devem ser exibidas como uma cadeia de eliminação com cada evento categorizado em estágios predefinidos.
- 8.1.2.6.28. Deve ter algoritmos preditivos para identificar usuários de risco (por exemplo, usuários prestes a deixar a organização);
- 8.1.2.6.29. Deve fornecer análises para diferentes tipos de anomalias, como relacionadas ao tempo, volume de transferência de dados, origem do evento relacionado, destino do evento relacionado, anomalias por usuário e grupo de pares, anomalias relacionadas a localização geográfica / velocidade terrestre, bem como rastrear usuários ou outras entidades nas listas de observação;
- 8.1.2.6.30. Deve ter algoritmos de aprendizagem não supervisionados para analisar eventos atuais e históricos e determinar associações, para estabelecer padrões de comportamento da atividade do usuário em cada fonte de evento por dia, semana, mês, hora do dia e dia da semana. Qualquer desvio do padrão regular deve ser marcado como uma anomalia;
- 8.1.2.6.31. Deve ter algoritmos de aprendizagem supervisionados para detectar ameaças de malware avançadas, como DGA, ataques de phishing/spam e muito mais;
- 8.1.2.6.32. Deve ter técnicas de análise baseadas pares para detectar usuários que estão começando a se comportar de maneira diferente dos pares, traçando o perfil do comportamento de diferentes usuários no grupo de pares e, em seguida, comparando as transações do usuário com a dos pares;
- 8.1.2.6.33. Deve haver técnicas de análise de raridade de eventos pelas quais atividades suspeitas que não foram vistas antes possam ser identificadas;
- 8.1.2.6.34. Deve ter técnicas de análise de comportamento por enumeração que permita criar linhas de base de eventos do mesmo tipo e procurar qualquer desvio do normal;
- 8.1.2.6.35. Deve ter técnicas de análise de tráfego para identificar padrões de beaconing, agentes de usuários incomuns, conexões com URLs incomuns, conexões com domínios DGA, etc;
- 8.1.2.6.36. Deve fornecer a capacidade de definir políticas baseadas em regras para detectar ameaças conhecidas. Essas ameaças conhecidas devem ser usadas como intensificadores de risco e combinadas com as verificações “não assinadas” nos modelos de ameaças;
- 8.1.2.6.37. Deve haver modelagem de ameaças que permita a identificação de ameaças compostas, que se observadas isoladamente podem ser de baixo risco, porém,

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

quando combinadas, são indicativas de um evento de alto risco;

- 8.1.2.6.38. Deve reduzir o número de falsos positivos aplicando recursos avançados de aprendizado de máquina para aprender o que é normal e o que não é normal no ambiente monitorado;
- 8.1.2.6.39. Deve ter relatórios de ameaças que forneçam visibilidade da postura de segurança cibernética. Por exemplo: usuários de alto risco, ativos de alto risco, principais ameaças, principais IPs maliciosas, etc;
- 8.1.2.6.40. Deve ter relatórios que forneçam visibilidade sobre as operações de segurança. Por exemplo, para dispositivos VPN, os relatórios devem incluir as melhores sessões de VPN por duração, os principais eventos de saída de dados, a distribuição dos eventos de login por geografia, as principais tentativas de login com falha e assim por diante;
- 8.1.2.6.41. Deve ter relatórios de conformidade alinhados com requisitos de conformidade específicos, como PCI, SOX, HIPPA, GDPR, ISO27002, etc;
- 8.1.2.6.42. Deve ter relatórios de resumo executivo de violações, incidentes e operações;
- 8.1.2.6.43. Deve ter relatórios sobre a atividade do usuário;
- 8.1.2.6.44. Deve permitir que os dados sejam exibidos com diferentes tipos de gráficos: gráfico de linhas, gráfico de barras, gráfico de pizza, mapa geográfico, tabelas, gráfico empilhados, gráfico N principais, gráficos de bolhas, gráficos de relacionamento de origem e destino;
- 8.1.2.6.45. Deve permitir a visualização de dados através de links que permitam vincular qualquer conjunto de atributos e visualização a relação entre eles;
- 8.1.2.6.46. O serviço deve possuir solução para análise de artefatos maliciosos que minimamente contemple as funcionalidades a seguir:
 - a) Analisar mais de 1000 indicadores comportamentais de um artefato;
 - b) Realizar análise estatística e dinâmica para avaliar se o artefato é malicioso ou não;
 - c) Deve suportar a análise dos artefatos BAT, CHM, DLL, ISO, HTA, HWP, JAR, JS, JSE, JTD, LNK, MSI, MHTML, documentos do Microsoft Office, EXE, PE32, PDF, VBE, URLs, WSF, XML e ZIP;

8.1.3. PROCESSOS A SEREM APLICADOS

8.1.3.1. PROCESSO DE MONITORAMENTO, DETECÇÃO E RESPOSTA

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 8.1.3.1.1. A CONTRATADA será responsável por implantar, operar e suportar toda a plataforma ofertada;
- 8.1.3.1.2. A fim de balizar todo o processo de monitoramento de ataques cibernéticos da CONTRATANTE, e influenciado pelos principais frameworks de boas práticas de serviços de segurança da informação, deverá ser desenhado/revisado em conjunto com a CONTRATANTE, o processo de resposta a incidentes focado em cibersegurança escopo desse contrato, que seja aderente as características específicas do ambiente da CONTRATANTE.
- 8.1.3.1.3. Após a definição/revisão e escrita da política de respostas a incidentes de cibersegurança, para início da implementação dos processos, deverá haver o aceite formal da CONTRATANTE.
- 8.1.3.1.4. É sabido que para o sucesso de um monitoramento de ataques cibernético, a primeira definição se deve a que tipo de ocorrência de eventos de segurança, se deseja detectar e tomar algum tipo de ação, logo será de responsabilidade da CONTRATADA como primeiro passo deste processo, a definição de linha de base de eventos monitorados.
- 8.1.3.1.5. Tal definição de linha de base de eventos de segurança monitorados, não deve ser tomada de forma unilateral pela CONTRATADA. A CONTRATANTE deverá participar ativamente no processo de construção de forma consultiva. Porém, se ratifica que é de responsabilidade da CONTRATADA a definição, e colocar em operação tal linha de base.
- 8.1.3.1.6. Espera-se que a linha de base de eventos de segurança monitorados, seja revista de forma mensal, contudo, não se limitando a este tempo, pois todos os dias novos ataques são projetados no mundo, e se espera que a CONTRATADA tome ciência destes ataques, e por sua vez atualize a linha de base, para que em um cenário onde estes novos ataques sejam direcionados a CONTRATANTE, sejam detectados através dos serviços em questão.
- 8.1.3.1.7. O produto de um evento é a correlação dos logs gerados pelos itens de configurações do parque da CONTRATANTE. Uma vez definida a linha de base de eventos, será também de responsabilidade da CONTRATADA avaliar se todos os insumos para a correta geração do evento, estão sendo enviados corretamente para a ferramenta.
- 8.1.3.1.8. Caso a CONTRATADA identifique a ausência dos insumos (eventos) a ser gerado por um item de configuração, será de reponsabilidade da CONTRATADA a correção e/ou habilitação de tal insumo dos itens de configuração descritos no tópico AMBIENTE TECNOLÓGICO DA CONTRATANTE (HARDWARE E SOFTWARE). Caso o item de configuração não pertencer ao objeto contratado, porém necessário para a correta geração do evento, deverá a CONTRATADA solicitar a CONTRATANTE a correção e/ou habilitação de tal insumo no item de

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

configuração em questão.

8.1.3.1.9. Dar-se-á então o passo de classificação do evento, também de responsabilidade da CONTRATADA. O grupo de monitoramento de ataques da CONTRATADA deve focar as ações nos eventos que são significativos. Logo, tal grupo deve analisar todos os eventos apresentados, classificando-os nos seguintes grupos, a saber:

- 8.1.3.1.9.1. Eventos de Informação: Estes eventos não requerem qualquer ação. São usados para fazer verificação de funcionalidade dos itens de configuração de segurança. Ou seja, tem por objetivo puro e simples, identificar se as ferramentas e soluções estão funcionando dentro do esperado. Estes eventos são também úteis para gerar estatísticas como, por exemplo, porcentagem de hosts com a última vacina de antivírus do dia.
- 8.1.3.1.9.2. Eventos de Aviso: Este grupo de eventos deve ser utilizado quando existe algum comportamento anômalo, se comparado a linha de base de operação padrão do ambiente (serviço ou solução), porém, ainda não gerou algum tipo de impacto ao ambiente (serviço ou solução) da CONTRATANTE, como por exemplo fictício: É esperado que exista 1.000 (mil) ataques do tipo port scan bloqueados pelo firewall, porém, na última hora, este número passou para 10.000 (dez mil) ataques, todavia, o firewall ainda continua bloqueando sem que haja degradação da performance do ambiente (serviço, tráfego e/ou solução).
- 8.1.3.1.9.3. Eventos de Exceção: Estes eventos são aqueles que sugere que os pilares de segurança da informação (confidencialidade, integridade e conformidade), foram impactados como, por exemplo: Uma infecção gerada por um malware do tipo ransomware, onde a mesma não tenha sido bloqueada pela solução de antivírus da CONTRATANTE. Este é o único tipo de evento que pode iniciar o processo de resposta a incidente de segurança, descrito no tópico, do presente termo de referência.
- 8.1.3.1.9.4. Uma vez classificado o evento, se inicia o passo de resposta ao mesmo, que também é de responsabilidade da CONTRATADA. As respostas a serem dadas a cada tipo de incidentes, serão baseadas na política de resposta a incidentes escrita previamente conforme descrito no presente termo.
- 8.1.3.1.9.5. Durante a fase de escrita e/ou definição dos processos a serem seguidos, deverá ser informado quais os respectivos tipos de ações para no mínimo os seguintes tipos de eventos:
- 8.1.3.1.9.6. Informacional;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 8.1.3.1.9.7. Aviso;
 8.1.3.1.9.8. Exceção;

8.1.3.1.10. Importante ressaltar que todo o processo de tratamento do evento, independente de qual fase e/ou status, deve ser registrado no módulo de tratamento de eventos da ferramenta. Também é responsabilidade da CONTRATADA a segurança dos eventos, e fica expressamente proibido a remoção de qualquer evento, independentemente de sua classificação e fase de tratamento, sem a autorização da contratante.

8.1.3.1.11. Deverá em conjunto com a CONTRATANTE, ser criado playbooks de resposta a incidentes.

8.1.4. GRUPO TÉCNICO DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS

- 8.1.4.1. Através do seu centro de operação de segurança, a CONTRATADA deverá manter uma torre de operação denominada GRUPO DE MONITORAMENTO DE ATAQUES, com objetivo e foco de trabalhar no processo de monitoramento de ataques cibernéticos.
- 8.1.4.2. Este grupo deverá ser exclusivo para trabalhar no serviço em questão, não podem os profissionais pertencentes a este grupo serem compartilhados e/ou atuarem, com os demais serviços descritos no objeto do presente termo de referência.
- 8.1.4.3. Todos os profissionais que integram GRUPO DE MONITORAMENTO DE ATAQUES, devem obrigatoriamente compor o quadro permanente de colaboradores da CONTRATADA em regime de trabalho CLT (Consolidação das Leis do Trabalho) ou contrato de prestação de serviços firmados diretamente entre esses profissionais e a CONTRATADA, sendo proibida a terceirização ou subcontratação de tal serviço.
- 8.1.4.4. Além dos profissionais que deverão ficar dedicados ao contrato conforme informado previamente no presente termo de referência o dimensionamento é de responsabilidade da CONTRATADA quantificar o número adequado de profissionais para a entrega de tal serviço, sem que haja impacto no acordo de nível de serviço estabelecido no tópico ACORDO DE NÍVEIS DE SERVIÇO do presente termo de referência.
- 8.1.4.5. A fim de garantir que os profissionais envolvidos tenham conhecimento e habilidade para executar o processo de monitoramento de ataques cibernéticos da CONTRATANTE, a CONTRATADA deverá, obrigatoriamente, compor o GRUPO DE MONITORAMENTO DE ATAQUES, com ao menos 01 (um) perfil de cada profissional que segue descrito abaixo:

Perfis	Certificações	Descrição
Analista de Segurança I	- CompTIA Security+ - CompTIA CySA+ - e/ou Certified Ethical Hacker	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

	Certificação em pelo menos uma das soluções escolhidas para atender o tópico SOBRE AS FERRAMENTAS A SEREM UTILIZADAS	Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.
Analista de Segurança II	- CompTIA Security+ e/ou CompTIA CySA+ e/ou - Certified Ethical Hacker	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de SIEM e ATD. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.

Tabela 2 - Certificações e qualificações do Grupo de Monitoramento de Ataques

8.1.4.6. Não existe restrição ou limite para acúmulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos no GRUPO DE MONITORAMENTO DE ATAQUES, porém, conforme já foi mencionado neste termo de referência, este(s) deve(m) compor única e exclusivamente o time denominado GRUPO DE MONITORAMENTO DE ATAQUES.

8.1.4.7. ENTREGAS A SEREM REALIZADAS

8.1.4.7.1. Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, o CONTRATANTE definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue de forma on line e em tempo de execução, através do portal de indicadores descrito no tópico de condições gerais para prestação do serviço deste termo de referência, a saber:

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Quantitativo de eventos correlacionados	Soma de eventos correlacionados	Eventos correlacionados	Eventos correlacionados	Número total de eventos correlacionados
Quantitativo de incidentes abertos	Soma de incidentes abertos	Incidentes abertos	Incidentes	Número total de incidentes abertos
Quantitativo de solicitações por grupo de tecnologia	Soma de solicitações relacionadas aos grupos de tecnologia	Solicitações relacionadas aos grupos de tecnologia	Solicitações	Número total de solicitações relacionadas por grupo de tecnologia
Quantitativo de regras de correlacionamento	Soma do número de regras de correlacionamento	Regras de correlacionamento	Regras de correlacionamento	Número total de regras de correlacionamento
TOP 10 – Regras de correlacionamento	Soma do número de eventos correlacionados por regra de correlacionamento	Eventos correlacionados	Regra de correlacionamento	TOP 10 do número de eventos correlacionados por regra de correlacionamento
TOP 10 – IP de destino de regras de correlacionamento	Soma do número de eventos correlacionados por IP de destino	Eventos correlacionados por IP de destino	IP de destino	TOP do número de eventos correlacionados por IP de destino
TOP 10 – Regras de correlacionamento por país de origem	Soma do número de eventos correlacionados por país de origem	Eventos correlacionados por país de origem	País de origem	TOP do número de eventos correlacionados por país de origem
TOP 10 – Tipos de ataques	Soma do número de ataques correlacionados por tipo de ataque	Eventos correlacionados por ataque	Ataques	TOP 10 por tipo de ataque

Tabela 3 - Indicadores Estratégicos de Monitoramento de Ataques Cibernéticos

9. SERVIÇO DE GESTÃO DE VULNERABILIDADES PARA 300 (TREZENTOS) ATIVOS

9.1. Tem por objetivo de forma proativa e recorrente, identificar possíveis vulnerabilidades de segurança da informação, na infraestrutura e aplicações do CONTRATANTE, identificando proativamente as vulnerabilidades de aplicações que seriam vetores de ataques, e tornando-as elegíveis de blindagem contra a exploração das vulnerabilidades identificadas afim de evitar que ataques cibernéticos direcionados ao CONTRATANTE, obtenha sucesso explorando tais vulnerabilidades já conhecidas.

9.2. SOBRE AS FERRAMENTAS A SEREM UTILIZADAS

9.2.1. ESPECIFICAÇÕES GERAIS

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 9.2.1.1. A solução deve realizar varreduras (*Scans*) de vulnerabilidades, avaliação de configuração e conformidade (*Baseline e Compliance*);
- 9.2.1.2. A solução deve possuir recurso de varredura ativa, onde o *Scanner* comunica-se com os alvos (ativos) através da rede;
- 9.2.1.3. A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT;
- 9.2.1.4. A solução deve ser licenciada pelo número de endereços IP ou dispositivos (*Assets*);
- 9.2.1.5. A solução deve fornecer um modelo de armazenamento integrado que não dependa de um banco de dados externos ou de terceiros;
- 9.2.1.6. Caso a solução dependa de banco de dados de terceiros, todas as licenças deverão ser fornecidas pela CONTRATADA.
- 9.2.1.7. A solução deverá suportar API (*Application Programming Interface*) baseada em REST (*Representational State Transfer*) para automação de processos e integração com aplicações terceiras.
- 9.2.1.8. A solução deve possuir integração via API no mínimo para as seguintes linguagens: *Python, Powershell, Ruby, Javascript, Java, Swift e PHP*;
- 9.2.1.9. A solução deve possuir métodos de consulta via API e envio, tais como: HTTP METHOD (POST, GET, PUT AND DELETE);
- 9.2.1.10. A solução deve incluir a opção para agentes instalados e licenciados em estações de trabalho e servidores para varredura diretamente no sistema operacional;
- 9.2.1.11. Tais agentes devem ser gerenciados pela mesma interface/console da plataforma de gestão de vulnerabilidades;
- 9.2.1.12. A solução deve permitir o agrupamento de *Scanners* para facilitar o gerenciamento e aplicação de políticas;
- 9.2.1.13. A solução deve realizar a varredura tanto de dispositivos na rede interna, dispositivos expostos a demais redes externas, tanto quanto dispositivos em nuvens públicas como Azure, AWS ou GCP;
- 9.2.1.14. O escaneamento para os dispositivos expostos deve ser realizados através de SCANS (ENGINE) do próprio fabricante alocados no Brasil;
- 9.2.1.15. Os Scanners e sensores agentes deverão ser gerenciados por uma única plataforma, de maneira centralizada;
- 9.2.1.16. O acesso a console de gerenciamento deve ser fornecida para pelo menos 10 usuários

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

simultâneos;

9.2.1.17. A solução deve ser capaz de se integrar e disponibilizar insumos para soluções de correlação de eventos externa (SIEM);

9.2.1.18. A solução deve apresentar, para cada vulnerabilidade encontrada, a descrição e passos que devem ser tomados para correção;

9.2.1.19. A solução deve apresentar, para cada vulnerabilidade encontrada, evidências da vulnerabilidade através de saídas das verificações (Outputs);

9.2.1.20. A solução deve fornecer controle de acesso baseado em função (RBAC- Role Based Access Control) para controlar o acesso do usuário a conjuntos de dados e funcionalidades;

9.2.1.21. A solução deve ser capaz de definir e gerenciar grupos de usuários, incluindo limitação de funções de varreduras e acesso a relatórios e Dashboards;

9.2.1.22. A solução deve ter a capacidade de excluir determinados endereços IP do escopo de qualquer varredura ou Scan;

9.2.1.23. A solução deve criptografar todos resultados de varreduras obtidos e informações inseridas tanto em descanso quanto em trânsito;

9.2.1.24. A solução deve suportar métodos de autenticação usando bases de autenticação local, e SAML (Security Assertion Markup Language) para uso de SSO (Single Sign-On);

9.2.1.25. A solução deve ser capaz de orquestrar Scanners ilimitados dentro da infraestrutura;

9.2.1.26. A solução não deve impor nenhum limite de quantidade de Scanners implementados dentro da infraestrutura;

9.2.1.27. A solução deverá possuir sistema de alertas para informar a disponibilidade de resultados dos escaneamentos através de Email;

9.2.1.28. A solução deve oferecer capacidade de configuração dinâmica de grupos de ativos através de no mínimo as seguintes características:

9.2.1.28.1. Sistema Operacional, Endereço IP, DNS, NetBIOS Host, MAC, AWS Instance Type, AWS EC2 Name, Software instalado, Azure VM ID, AWS Region, Google Cloud Instance ID, Azure Resource ID, Ativos avaliados;

9.2.2. Dos requisitos e relatórios e painéis gerenciais

9.2.2.1. A solução deverá possuir painéis gerenciais (Dashboards) pré-definidos para rápida visualização dos resultados, permitindo ainda a criação de painéis personalizados;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 9.2.2.2. Os painéis gerenciais deverão ser apresentados em diversos formatos, incluindo gráficos e tabelas, possibilitando a exibição de informações em diferentes níveis de detalhamento;
- 9.2.2.3. Os relatórios devem ser disponibilizados sob demanda no console de gerência da solução;
- 9.2.2.4. Os relatórios devem conter informações da vulnerabilidade, severidade, se existe um Exploit disponível e informações do ativo;
- 9.2.2.5. A solução deve permitir a customização de Dashboards/relatórios;
- 9.2.2.6. A solução deve concentrar todos os relatórios na plataforma central de gerenciamento, não sendo aceitas soluções fragmentadas;
- 9.2.2.7. A solução deve ser capaz de produzir relatórios, pelo menos, nos seguintes formatos: HTML, PDF e CSV;
- 9.2.2.8. A solução deve possibilitar a criação de relatórios baseado nos seguintes alvos: Todos os ativos e Alvos específicos;
- 9.2.2.9. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável);
- 9.2.2.10. A solução deve suportar o envio automático de relatórios para destinatários específicos;
- 9.2.2.11. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;
- 9.2.2.12. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;
- 9.2.3. Das varreduras
 - 9.2.3.1. A solução deve realizar varreduras em uma variedade de sistemas operacionais, incluindo, no mínimo, Windows, Linux e Mac OS, bem como Appliances virtuais;
 - 9.2.3.2. A solução deve suportar varredura com e sem agente, de maneira ativa e passiva, distribuídas em diferentes localidades e regiões e gerenciar todos por uma console central;
 - 9.2.3.3. A solução deve fornecer agentes instaláveis em sistemas operacionais distintos para monitoramento contínuo de vulnerabilidades;
 - 9.2.3.4. Tais agentes devem realizar conexões para o sistema gerenciamento através de protocolo seguro;
 - 9.2.3.5. A solução deve ser configurável para permitir a otimização das configurações de varredura;
 - 9.2.3.6. A solução deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 9.2.3.7. A solução deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;
- 9.2.3.8. A solução deve se integrar com solução de gerenciamento de acessos privilegiados para autenticação nos dispositivos, no mínimo, os seguintes:
- 9.2.3.8.1. CyberArk;
 - 9.2.3.8.2. BeyondTrust;
 - 9.2.3.8.3. Thycotic;
 - 9.2.3.8.4. Centrify;
- 9.2.3.9. A solução deve suportar o agendamento de *Scans* personalizados, incluindo a capacidade de executar varreduras em tempos designados, com frequência pré-determinada;
- 9.2.3.10. A solução deve ser capaz de identificar novos *hosts* no ambiente sem a necessidade de *Scan*;
- 9.2.3.11. A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;
- 9.2.3.12. A solução deve ser capaz de realizar em tempo real a descoberta de vulnerabilidades nas seguintes tecnologias:
- 9.2.3.12.1. Cloud Services;
 - 9.2.3.12.2. Data Leakage;
 - 9.2.3.12.3. Database;
 - 9.2.3.12.4. IoT;
 - 9.2.3.12.5. Mobile Devices;
 - 9.2.3.12.6. Operating System;
 - 9.2.3.12.7. Peer-To-Peer;
 - 9.2.3.12.8. Web Servers;
 - 9.2.3.12.9. Web Clients.
- 9.2.3.13. A solução deve ser capaz de identificar a comunicação de malwares na rede de forma passiva;
- 9.2.3.14. A solução deve, em tempo real, detectar Logins e Downloads de arquivos em um compartilhamento de rede;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

9.2.4. Da análise e priorização de vulnerabilidades

9.2.4.1. A solução deve ser capaz de exibir ambos severidade e pontuação, com base em CVSS (Common Vulnerability Scoring System) e inteligência de ameaças;

9.2.4.2. A solução deve utilizar sistema de pontuação e priorização das vulnerabilidades que utilize no mínimo:

9.2.4.2.1. CVSS Impact Score;

9.2.4.2.2. Idade da Vulnerabilidade;

9.2.4.2.3. Maturidade de códigos de exploração da vulnerabilidade encontrada;

9.2.4.2.4. Frequência de uso da vulnerabilidade em ataques e campanhas atuais;

9.2.4.2.5. Disponibilidade do código de exploração da vulnerabilidade;

9.2.4.2.6. Presença de módulos de exploração de vulnerabilidade em Frameworks automatizados de exploração de vulnerabilidades como CANVAS, Metasploit e Core Impact;

9.2.4.2.7. Popularidade da vulnerabilidade em fóruns e comunicações na *Darkweb*;

9.2.4.2.8. O mecanismo de priorização deve ser sujeito a modificações e atualizações diárias com base em inteligência de ameaças e observação de tendências na *Internet*;

9.2.5. Da Análise de Risco do Ambiente

9.2.5.1. A solução deve gerar um Score que combine dados de vulnerabilidades com a criticidade dos ativos do ambiente computacional;

9.2.5.2. O Score deve ser gerado automaticamente por meio de algoritmos de inteligência artificial (Machine Learning) e deve calcular a probabilidade de exploração de uma determinada vulnerabilidade;

9.2.5.3. Deve ser capaz de calcular a criticidade dos ativos da organização;

9.2.5.4. A solução deve ser capaz de realizar um Benchmark no ambiente da CONTRATANTE comparando sua maturidade com outras organizações do mesmo setor;

9.2.5.5. A solução deve prover visão sobre quais ações de remediação reduzem o maior nível de risco do ambiente;

9.2.5.6. A solução deve também permitir a visualização de ações de remediação agregadas para visão consolidada de redução de risco;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 9.2.5.7. Deve permitir modificar a qualquer momento o tipo de indústria para comparação. Ex: Mudar de Setor Público para Mercado Financeiro;
- 9.2.5.8. Deve fornecer uma lista com as principais recomendações para o ambiente com foco na redução da exposição cibernética da organização;
- 9.2.5.9. A solução deve gerar uma pontuação para cada um dos ativos onde é levado em conta as vulnerabilidades presentes naquele ativo assim como a classificação do ativo na rede (peso do ativo);
- 9.2.5.10. A solução deve gerar uma pontuação global referente a exposição cibernética da organização baseado nas pontuações de cada um dos ativos;
- 9.2.5.11. A solução deve oferecer uma capacidade de comparação (Benchmarking) da pontuação referente a exposição cibernética com outros Players da mesma indústria assim como outras empresas do mercado;
- 9.2.5.12. A solução deve permitir um acompanhamento histórico do nível de exposição da organização;
- 9.2.5.13. Permitir realizar alterações na classificação dos ativos (atribuição de pesos diferentes) podendo sobrescrever a classificação atribuída automaticamente pela solução;
- 9.2.5.14. A solução deverá apresentar indicadores específicos referentes a remediação, possuindo no mínimo informações referentes ao tempo entre remediação e o tempo o qual a vulnerabilidade foi descoberta no ambiente, tempo entre a remediação e a data de publicação da vulnerabilidade, quantidade média de vulnerabilidades críticas por ativo e a comparação da quantidade de vulnerabilidades corrigidas por criticidade;
- 9.2.5.15. A solução deve permitir a segregação lógica entre áreas distintas da empresa a fim de obter a pontuação referente exposição cibernética por área;
- 9.2.6. Da descoberta de Ativos:
- 9.2.6.1. A solução deve ser capaz de realizar escaneamento de descoberta de rede utilizando os seguintes critérios como alvo: IP, CIRD e Range;
- 9.2.6.2. A solução deve disponibilizar modelos de escaneamento de descoberta, ajustável, com os seguintes tipos de scan:
- 9.2.6.2.1. Enumeração de Hosts;
 - 9.2.6.2.2. Identificação de Sistema Operacional (SO);
 - 9.2.6.2.3. Port Scan (Portas comuns);
 - 9.2.6.2.4. Port Scan (Todas as portas);

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

9.2.6.2.5. Customizado;

9.2.6.3. A solução deve permitir realizar escaneamento de descoberta customizado podendo ser parametrizado de acordo com a necessidade;

9.2.6.4. A parametrização do escaneamento de descoberta deve, no mínimo, conter os seguintes requisitos:

9.2.6.4.1. Descoberta de Host;

9.2.6.4.2. Ping o host remoto;

9.2.6.4.3. Usar descoberta rápida;

9.2.6.4.4. Métodos de ping;

9.2.6.4.4.1. ARP;

9.2.6.4.4.2. TCP;

9.2.6.4.4.3. ICMP;

9.2.6.4.4.4. UDP;

9.2.6.4.5. Escaneamento de descoberta em redes de impressora;

9.2.6.4.6. Escaneamento em redes Novell;

9.2.6.4.7. Tecnologia de Wake-on-LAN;

9.2.6.5. Port Scanning:

9.2.6.5.1. Portas;

9.2.6.5.1.1. Considerar portas não escaneadas como fechadas;

9.2.6.5.1.2. Range de portas a serem escaneadas;

9.2.6.6. Enumerar Portas locais:

9.2.6.6.1. SSH (netstat);

9.2.6.6.2. WMI (netstat);

9.2.6.6.3. SNMP;

9.2.7. Da descoberta de serviços

9.2.7.1. Sondar todas as portas para encontrar serviços;

9.2.7.2. Procurar por serviços baseado em SSL/TLS;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

9.2.7.3. Enumerar todas as cifras SSL/TLS;

9.2.8. A solução deve realizar descoberta de ativo de forma passiva e adicionado automaticamente na console de gerenciamento;

9.2.9. A solução deve descobrir passivamente quando um *host* é adicionado na rede;

9.2.10. Da avaliação de vulnerabilidade

9.2.10.1. A solução deve ser capaz de realizar testes sem a necessidade de agentes instalados no dispositivo destino para detecção de vulnerabilidades;

9.2.10.2. A solução deve detectar e classificar através de severidades, riscos e vulnerabilidades;

9.2.10.3. A solução deve também fornecer informações detalhadas sobre a natureza da vulnerabilidade, evidências da existência da vulnerabilidade e recomendações para mitigá-los;

9.2.10.4. A solução deve incluir uma saída detalhada das vulnerabilidades descobertas como versões de DLL esperadas e encontradas;

9.2.10.5. A solução deve ser compatível com CVE e fornecer pelo menos 10 anos de cobertura CVE;

9.2.10.6. A solução deve identificar vulnerabilidades específicas para o *Active Directory* com os seguintes padrões de verificação;

9.2.10.6.1. Contas administrativas vulneráveis a *Kerberoasting Attack*;

9.2.10.6.2. Utilização de criptografia vulnerável com autenticação *Kerberos*;

9.2.10.6.3. Contas com pré-autenticação do *Kerberos* desabilitada;

9.2.10.6.4. Verificação de usuários com a opção de nunca expirar a senha com a opção habilitada;

9.2.10.6.5. Verificar validação de fragilidades do tipo “Unconstrained Delegation”;

9.2.10.6.6. Verificação de “Pre-Windows 2000 Compatible Access”;

9.2.10.6.7. Verificação de validade de chaves mestras “Kerberos KRBTGT”;

9.2.10.6.8. Verificação de “SID History Injection”;

9.2.10.6.9. Verificação de “Printer Bug Exploit”;

9.2.10.6.10. Verificação de “Primary Group ID”;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

9.2.10.6.11. Verificação de usuários com *Passwords* em branco;

- 9.2.10.7. A solução deve suportar o uso de SMB e WMI para verificação de sistemas Microsoft Windows;
- 9.2.10.8. A solução deve ser capaz de iniciar automaticamente serviços de registro remoto em sistemas Windows ao executar uma varredura credenciada;
- 9.2.10.9. A solução deve ser capaz de parar automaticamente o serviço de registro remoto em sistemas Windows novamente assim que a varredura estiver completa;
- 9.2.11. O Scanner deve oferecer suporte a Shell seguro (SSH) com a capacidade de escalar privilégios para varredura de vulnerabilidades e auditorias de configuração em sistemas Unix;
- 9.2.11.1. A solução deve suportar o uso do Netstat (Linux) e WMI (Windows) para uma enumeração rápida e precisa de portas em um sistema quando as credenciais são fornecidas;
- 9.2.11.2. A solução deve possibilitar a verificação remota de portas, além da enumeração local de portas, para ajudar a determinar se algum mecanismo de controle de acesso está sendo utilizado;
- 9.2.11.3. A solução deve fornecer auditoria de Patch (MS Bulletins) para as principais versões de Windows;
- 9.2.11.4. A solução deve fornecer auditoria de Patch para todos os principais sistemas operacionais Unix incluindo Mac OS, Linux, Solaris e IBM AIX;
- 9.2.11.5. A solução deve fornecer varredura para aplicativos comerciais diversos e proprietários, incluindo, mas não limitando-se a: Java, Adobe, Oracle, Apple, Microsoft, Check Point, Palo Alto Networks, Cisco, Fortinet, Fireeye, McAfee, etc;
- 9.2.11.6. A solução deve incluir classificação de severidades de acordo com o padrão Sistema Comum de Pontuação de Vulnerabilidade Versão (CVSS2 e CSVSS 3);
- 9.2.11.7. A solução deve fornecer informações acerca da disponibilidade de códigos de exploração das vulnerabilidades encontradas em Frameworks de exploração para as plataformas mais populares: Core, Metasploit e Canvas;
- 9.2.11.8. A solução deve informar se a vulnerabilidade pode e está sendo ativamente explorada por código malicioso (Malware);
- 9.2.11.9. A solução deve possuir importação de arquivos .YARA;
- 9.2.11.10. Deve ser capaz de identificar e classificar vulnerabilidades de máquinas virtuais em nuvem pública em infraestruturas como serviço nas plataformas AWS, Microsoft Azure e Google Cloud;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

9.2.12. Da auditoria de Configuração

9.2.12.1. A solução deve ser capaz de realizar auditoria de conformidade sem a necessidade de agente instalado no dispositivo de destino;

9.2.12.2. A solução deve fornecer *Benchmarks* de auditoria de segurança e configuração para conformidade regulatória e outros padrões de práticas recomendadas pela área ou fabricantes;

9.2.12.3. A solução deve realizar verificações de auditoria contendo as de segurança, com indicação de sucesso ou falha, baseado nos principais *Frameworks* reconhecidos pela indústria, pelo menos os seguintes:

9.2.12.3.1. *Center for Internet Security Benchmarks* (CIS);

9.2.12.3.2. *Defense Information Systems Agency* (DISA) STIGs;

9.2.12.3.3. *Health Insurance Portability and Accountability Act* (HIPAA);

9.2.12.3.4. *Payment Card Industry Data Security Standards* (PCI DSS);

9.2.12.4. A solução deve fornecer auditoria de programas antivírus para determinação de presença e *Status* de inicialização para no mínimo os seguintes produtos: TrendMicro Office Scan, McAfee VirusScan, Microsoft Endpoint Protection e Kaspersky;

9.2.12.5. A solução deve fornecer auditorias de configuração com base *Benchmarks* em CIS (*Center for Internet Security*) L1 e L2, para ambos os sistemas operacionais Microsoft Windows e Linux;

9.2.12.6. A solução deve permitir auditoria de conformidade em servidores Windows, Linux, Bancos de Dados SQL Server, a fim de determinar se estão configurados de acordo com os principais Framework de segurança como, por exemplo, CIS e DISA;

9.2.12.7. A solução deve oferecer validação e suporte a SCAP (*Security Content Automation Protocol*);

9.2.13. Análise dinâmica de vulnerabilidades para aplicações Web

9.2.13.1. A solução deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web como parte dos ativos a serem inspecionados;

9.2.13.2. A solução deve ser capaz de executar varreduras em sistemas web através de seus endereços IP ou FQDN (DNS);

9.2.13.3. A solução deve avaliar no mínimo os padrões de segurança OWASP Top 10 e PCI (*Payment Card Industry Data Security Standard*);

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 9.2.13.4. A solução deve suportar as diretivas PCI ASV 5.5 para definição de escopo de análise da aplicação;
- 9.2.13.5. A solução deve suportar as diretivas PCI ASV 6.1 para definição de balanceadores de carga das aplicações bem como suas configurações para inclusão no relatório de resultados;
- 9.2.13.6. A solução deve possuir *Templates* prontos de varreduras entre simples e extensos;
- 9.2.13.7. Para varreduras extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos:
- 9.2.13.7.1. *Cookies, Headers, Formulários e Links*;
 - 9.2.13.7.2. Nomes e valores de parâmetros da aplicação;
 - 9.2.13.7.3. Elementos JSON e XML;
 - 9.2.13.7.4. Elementos DOM;
- 9.2.13.8. A solução deve permitir somente a execução da função *Crawler*, que consiste na navegação para descoberta das URLs existentes na aplicação;
- 9.2.13.9. A solução deve ser capaz de utilizar *Scripts* customizados de *Crawl* com parâmetros definidos pelo usuário;
- 9.2.13.10. A solução deve excluir determinadas URLs da varredura através de expressões regulares;
- 9.2.13.11. A solução deve excluir determinados tipos de arquivos através de suas extensões;
- 9.2.13.12. A solução deve instituir no mínimo os seguintes limites:
- 9.2.13.12.1. Número máximo de URLs para *Crawl* e navegação;
 - 9.2.13.12.2. Número máximo de diretórios para varreduras;
 - 9.2.13.12.3. Número máximo de elementos DOM;
 - 9.2.13.12.4. Tamanho máximo de respostas;
 - 9.2.13.12.5. Limite de requisições de redirecionamentos;
 - 9.2.13.12.6. Tempo máximo para a varredura;
 - 9.2.13.12.7. Número máximo de conexões HTTP ao servidor hospedando a aplicação Web;
 - 9.2.13.12.8. Número máximo de requisições HTTP por segundo.
- 9.2.13.13. A solução deve detectar congestionamento de rede e limitar os seguintes aspectos da

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

varredura:

- 9.2.13.13.1. Limite em segundos para *Timeout* de requisições de rede;
- 9.2.13.13.2. Número máximo de *Timeouts* antes que a varredura seja abortada;
- 9.2.13.14. A solução deve agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;
- 9.2.13.15. A solução deve enviar notificações através de no mínimo *E-mail* e SMS;
- 9.2.13.16. A solução deve possuir a flexibilidade de selecionar quais testes serão realizados de forma granular, através da seleção de testes, *Plug-ins* ou ataques;
- 9.2.13.17. A solução deve avaliar sistemas web utilizando protocolos HTTP e HTTPS;
- 9.2.13.18. A solução deve possibilitar a definição de atributos no cabeçalho (*HEADER*) da requisição HTTP de forma personalizado a ser enviada durante os testes;
- 9.2.13.19. A solução deve ser compatível com avaliação de *Web Services* REST e SOAP;
- 9.2.13.20. Deverá suportar no mínimo os seguintes esquemas de autenticação:
 - 9.2.13.20.1. Autenticação básica (*Digest*);
 - 9.2.13.20.2. NTLM;
 - 9.2.13.20.3. *Form de Login*;
 - 9.2.13.20.4. Autenticação de *Cookies*;
 - 9.2.13.20.5. Autenticação através de *Selenium*;
 - 9.2.13.20.6. Autenticação através de *Bearer*;
- 9.2.13.21. A solução deve importar *Scripts* de autenticação *Selenium* previamente configurados pelo usuário;
- 9.2.13.22. A solução deve customizar parâmetros *Selenium* como *Delay* de exibição da página, *Delay* de execução de comandos e *Delay* de comandos para recepção de novos comandos;
- 9.2.13.23. A solução deve exibir os resultados das varreduras em tendência temporal para acompanhamento de correções e introdução de novas vulnerabilidades;
- 9.2.13.24. A solução deve exibir os resultados agregados de acordo com as categorias do OWASP Top 10 (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project);

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

9.2.13.25. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;

9.2.13.26. Para cada vulnerabilidade encontrada, deve ser exibido evidências da mesma em seus detalhes;

9.2.13.27. Para vulnerabilidades de injeção de código (SQL, XSS, XSRF etc.), deve evidenciar nos detalhes do evento encontrado:

9.2.13.27.1. *Payload* injetado;

9.2.13.27.2. Evidência em forma de resposta da aplicação;

9.2.13.27.3. Detalhes da requisição HTTP;

9.2.13.27.4. Detalhes da resposta HTTP;

9.2.13.28. Os detalhes das vulnerabilidades devem conter descrição da falha e referências didáticas para a revisão dos analistas;

9.2.13.29. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação das mesmas;

9.2.13.30. A solução deve possuir suporte a varreduras de componentes para no mínimo:

9.2.13.30.1. Wordpress, Blog Designer Plugin for Wordpress, Event Calendar Plugin for Wordpress, Convert Plus Plugin for Wordpress, AngularJS, Apache, Apache Tomcat, Apache Tomcat JK connecto, Apache Spark e Apache Struts, Atlassian Confluence, Atlassian Crowd e Atlassian Jira, Backbone.js, ASP.NET, Bootstrap, Drupal, Joomla!, jQuery, Lighttpd, Magento, Modernizr, Nginx, PHP, AJAX, Sitefinity, Telerik, ThinkPHP, Webmin e YUI;

9.2.14. Solução de análise de infraestrutura sobre código em ambiente de Imagens em Contêiner, DevOps e GitOps.

9.2.14.1. A solução deve detectar e configurações incorretas da infraestrutura de nuvem em fases de design, construção e tempo de execução do seu ciclo de vida de desenvolvimento de software;

9.2.14.2. A solução deve prevenir problemas de segurança identifique e remova falhas na nuvem durante desenvolvimento antes de chegarem à produção;

9.2.14.3. A solução deve ser possível avaliar modelos de infraestrutura como código (IaC), com integrações nativas em:

9.2.14.3.1.1. Terraform;

9.2.14.3.1.2. AWS CloudFormation;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

9.2.14.3.1.3. Azure Resource Manager;

9.2.14.3.1.4. Kubernetes;

9.2.14.4. A solução deve prevenir o desvio de postura na nuvem identifique discrepâncias entre o IaC e sua nuvem em execução ambiente;

9.2.14.5. A solução deve fornecer sugestões de correção automaticamente por meio de pull ou mesclagem;

9.2.14.6. A solução deve contextualizar riscos compreender as vulnerabilidades de aplicativos no contexto de suas configurações de infraestrutura para obter uma imagem real do risco que eles presente;

9.2.14.7. A solução deve prover integração no mínimo com as seguintes plataformas abaixo:

9.2.14.7.1.1. Jira;

9.2.14.7.1.2. Slack;

9.2.14.7.1.3. AWS SNS;

9.2.14.7.1.4. Jenkins;

9.2.14.7.1.5. Terraform Cloud;

9.2.14.7.1.6. CircleCI;

9.2.14.7.1.7. Splunk;

9.2.14.7.1.8. AWS CloudTrail;

9.2.14.8. A solução deve possuir integração com no mínimo os seguintes Repositórios:

9.2.14.8.1.1. Bitbucket;

9.2.14.8.1.2. GitHub;

9.2.14.8.1.3. GitLab;

9.2.14.8.1.4. Azure DevOps;

9.2.14.9. A solução deve possuir funcionalidade de monitoramento dos repositórios sempre que houver alteração de código uma verificação automática via IaC deve apresentar a diferença;

9.2.14.10. A solução deve possuir políticas de análise em ambiente de nuvem para no mínimo as seguintes plataformas:

9.2.14.10.1.1. AWS;

9.2.14.10.1.2. Azure;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 9.2.14.10.1.3. GCP;
- 9.2.14.10.1.4. Kubernetes;

9.2.15. A solução deve possuir análise por benchmarks e compliance para os seguintes padrões em formato de Dashboard:

- 9.2.15.1. CIS;
- 9.2.15.2. NIST;
- 9.2.15.3. ISO-27001;
- 9.2.15.4. HIPAA;
- 9.2.15.5. PCI-DSS;
- 9.2.15.6. CCM;
- 9.2.15.7. GDPR;
- 9.2.15.8. A solução deve analisar, testar e reportar falhas de segurança em aplicações em Containers Docker como parte dos ativos a serem inspecionados;
- 9.2.15.9. A solução deve ser capaz de analisar imagens preparadas pelos desenvolvedores na esteira DevOps em busca de imagens com vulnerabilidades identificadas e malware residente no sistema de arquivos;
- 9.2.15.10. A solução deve integrar a esteira DevOps através de API, invocando o envio da imagem para análise em repositório próprio da solução ou utilizando scanner implementado em infraestrutura proprietária do órgão com a finalidade de evitar o envio de imagens e propriedade intelectual da contratante;
- 9.2.15.11. A documentação de API da solução deverá ter acesso público através de website ou documentação do próprio fabricante;
- 9.2.15.12. A console de administração deverá possuir controle de acesso no mínimo permitindo usuários com capacidade de somente visualizar as informações, e usuários com capacidade para efetuar análise das imagens;
- 9.2.15.13. A solução deve inventariar o sistema operacional de cada imagem analisada e suas vulnerabilidades encontradas;
- 9.2.15.14. A solução deve identificar containers que não foram analisados antes de sua implementação em produção;
- 9.2.15.15. A solução deve analisar as camadas (layers) de um container;
- 9.2.15.16. A solução deve identificar containers que tiveram mudanças de arquivos entre a análise

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

e a sua implementação em produção;

9.2.15.17. A solução deve informar os CVEs para cada vulnerabilidade encontrada nos pacotes e bibliotecas residentes na imagem;

9.2.15.18. A solução deve ter a capacidade de testar automaticamente todas as imagens armazenadas, ou previamente testadas, sempre que uma nova vulnerabilidade for publicada e atualizada no banco de dados de vulnerabilidade da solução, sem qualquer tipo intervenção manual;

9.2.15.19. A solução deve inventariar os pacotes e bibliotecas e suas respectivas versões e listar as mesmas dentro do relatório de resultados de análise de cada imagem;

9.2.15.20. A solução deve possuir conectores e permitir importação de imagens dos seguintes repositórios:

- 9.2.15.20.1.1. - Docker;
- 9.2.15.20.1.2. - Docker EE;
- 9.2.15.20.1.3. - AWS ECR;
- 9.2.15.20.1.4. - JFrog Artifactory;

9.2.15.21. A solução deve possuir integração com Microsoft Azure Container, Vmware Harbor e Sonatype Nexus para importar e analisar imagens;

9.2.15.22. A solução deve fornecer scanner em formato Docker para implementação local e análise de imagens sem a necessidade de envio destas para repositório remoto, fora do ambiente da contratante;

9.2.15.23. A solução ser capaz de configurar políticas usando como condições: CVSS Score, CVEs específicos e Malware identificado;

9.2.15.24. A solução deve permitir a criação de políticas específicas por repositório;

9.2.15.25. A solução deve prover integração com as seguintes plataformas de integração contínua: Bamboo, CircleCI, Codeship, Distelli, Drone.io, Jenkins, Shippable, Solano Labs, Travis CI, Wrecker e Kubernetes;

9.2.16. Da Análise em ambiente Microsoft *Active Directory*

9.2.16.1. A solução deve identificar fraquezas ocultas em configurações dedicadas ao *Active Directory*;

9.2.16.2. A solução deve possuir ações preventivas de *Hardening* para o *Active Directory*;

9.2.16.3. A solução deve identificar ataque específicos para a estrutura do *Active Directory*;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 9.2.16.4. A solução deve possuir funcionalidade para analisar em detalhes cada configuração incorreta que acarreta riscos de segurança – com uma linguagem simples, contextualizando tal risco para os times envolvidos;
- 9.2.16.5. A solução deve possuir recomendações de correção para cada configuração incorreta no *Active Directory*;
- 9.2.16.6. A solução deve avaliar relações de confiança perigosas entre florestas e domínios;
- 9.2.16.7. A solução deve capturar as mudanças que ocorrem no AD e demonstrar na console de administração;
- 9.2.16.8. A solução deve possuir *Dashboard* com os principais ataques e vulnerabilidades por domínio;
- 9.2.16.9. A solução deve permitir a correlação de mudanças no *Active Directory* e desvios de segurança;
- 9.2.16.10. A solução deve analisar em detalhes um ataque explorando as descrições através do *Framework* MITRE ATT&CK;
- 9.2.16.11. A solução deve prover interface web para gerenciamento de todas as funcionalidades;
- 9.2.16.12. A solução deve possuir capacidade nativa de criação de *Dashboards* customizados;
- 9.2.16.13. A solução deve suportar um modelo de controle de acesso baseado em funções (RBAC) flexível;
- 9.2.16.14. A solução deve realizar alterações no *Active Directory*, seus objetos e atributos;
- 9.2.16.15. A solução deve armazenar ou sincronizar nenhuma credencial de objetos do *Active Directory*;
- 9.2.16.16. A solução deve suportar ambientes com múltiplas florestas e domínios;
- 9.2.16.17. A solução deve suportar monitoramento contínuo de ambientes com *Active Directory* com o nível funcional de floresta e domínio a partir do 2003;
- 9.2.16.18. A solução deve suportar e reter os eventos coletados por no mínimo um ano;
- 9.2.16.19. A solução deve descobrir e mapear a superfície de ataque do *Active Directory* e seus domínios monitorados com os seguintes padrões:
- 9.2.16.19.1.1. Não depender de agentes ou sensores para coleta de informações do AD;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

9.2.16.19.1.2. A solução deve seguir as boas práticas de *menor privilégio*, a conta de serviço utilizada para conexão com o *Active Directory*, sendo o menor nível de acesso esperado para a conta de serviço como parte do grupo *Domain User*;

9.2.16.19.1.3. Interface web que consolida e apresenta de maneira unificada os domínios monitorados e as possíveis relações de confiança estabelecidas entre eles;

9.2.16.20. A solução deve analisar continuamente a postura de segurança do AD, minimamente avaliando:

9.2.16.20.1. Validação de GPOs desvinculadas, desabilitadas ou órfãs;

9.2.16.20.2. Validação de contas desativadas em grupos privilegiados;

9.2.16.20.3. Domínio usando uma configuração perigosa de compatibilidade com versões anteriores por meio de alterações no atributo *dSHeuristics*;

9.2.16.20.4. Validação de atributos relacionados a roaming de credenciais vulneráveis (*ms-PKI-DPAPIMasterKeys*) gerenciados por um usuário sem privilégios;

9.2.16.20.5. Validação de domínio sem GPOs de proteção de computador, desativando protocolos vulneráveis antigos, como *NTLMv1*;

9.2.16.20.6. Validação de contas com senhas que nunca expiram;

9.2.16.20.7. Validação de senhas reversíveis em GPOs;

9.2.16.20.8. Validação de uso de senhas reversíveis em contas de usuário;

9.2.16.20.9. Validação de utilização de protocolo criptográfico fraco (Ex. DES) em contas de usuário;

9.2.16.20.10. Validação de uso do LAPS (Solução de senha de administrador local) para gerenciar senhas de contas locais com privilégios;

9.2.16.20.11. Validação se o domínio possui um nível funcional desatualizado;

9.2.16.20.12. Validação de contas de usuário utilizando senha antiga;

9.2.16.20.13. Validação se o atributo *AdminCount* está definido em usuários padrão;

9.2.16.20.14. Validação do uso recente da conta de administrador padrão;

9.2.16.20.15. Validação de usuários com permissão para ingressar computadores no domínio;

9.2.16.20.16. Validação de contas dormentes;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 9.2.16.20.17. Validação de computadores executando um sistema operacional obsoleto;
- 9.2.16.20.18. Validação de restrições de *Logon* para usuários privilegiados em ambiente com múltiplos *Tiers* (1, 2 e 3) de segregação de ativos;
- 9.2.16.20.19. Validação de direitos perigosos configurados no *Schema* do AD;
- 9.2.16.20.20. Validação de relação de confiança perigosa com outras *Florestas* e *Domínios*;
- 9.2.16.20.21. Validação de contas que possuem um atributo perigoso de histórico SID (*SID History*);
- 9.2.16.20.22. Validação de contas utilizando controle de acesso compatível com versões anteriores ao Windows 2000;
- 9.2.16.20.23. Validação da última alteração de senha do KDC;
- 9.2.16.20.24. Validação da última alteração da senha da conta SSO do *Azure AD*;
- 9.2.16.20.25. Validação de contas que podem ter senha em branco/vazia;
- 9.2.16.20.26. Validação de utilização do grupo nativo *Protected Users*;
- 9.2.16.20.27. Validação de privilégios sensíveis (Ex. *Debug a program*, *Replace a process level token*, etc.) perigosos atribuídos aos usuários;
- 9.2.16.20.28. Validação de possível senha em *Clear-Text*;
- 9.2.16.20.29. Validação de sanidade das GPOs e componentes CSEs (*Client-Side Extension*);
- 9.2.16.20.30. Validação de uso de algoritmos de criptografia fracos na PKI do *Active Directory*;
- 9.2.16.20.31. Validação de contas de serviço com SPN (*Service Principal Name*) que fazem parte de grupos privilegiados;
- 9.2.16.20.32. Validação de contas anormais nos grupos administrativos padrão do AD;
- 9.2.16.20.33. Validação de consistência no *container adminSDHolder*;
- 9.2.16.20.34. Validação de delegação *Kerberos* perigosa;
- 9.2.16.20.35. Validação em permissões de objetos raiz que permitem ataques do tipo DCSync;
- 9.2.16.20.36. Validação de políticas de senha fracas aplicadas aos usuários;
- 9.2.16.20.37. Validação das permissões relacionadas às contas do *Azure AD Connect*;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 9.2.16.20.38. Validação do ID do grupo primário do usuário (*Primary Group ID*);
- 9.2.16.20.39. Validação de permissões em GPOs sensíveis associadas aos *Containers Configuration*, *Sites*, *Root Partition* e *OUs* sensíveis como *Domain Controllers*;
- 9.2.16.20.40. Controladores de domínio gerenciados por usuários ilegítimos;
- 9.2.16.20.41. Validação de certificado mapeado através de atributo *altSecurityIdentities* em contas privilegiadas;
- 9.2.16.20.42. Validação de uso de protocolo *Netlogon* inseguro (*ZeroLogon/CVE-2020-1472*);
- 9.2.16.21. A solução deve identificar vulnerabilidades e configurações incorretas do AD à medida que são introduzidas sendo:
- 9.2.16.21.1. Identificar todas as vulnerabilidades e configurações incorretas no AD;
 - 9.2.16.21.2. Monitorar relações de confiança perigosas em toda a estrutura AD;
 - 9.2.16.21.3. Apresentar ameaças e alterações sem a necessidade de *Scans* estáticos e programados no *Active Directory* e sua infraestrutura;
 - 9.2.16.21.4. Apresentar as ameaças e alterações em tempo real ou em menos de cinco minutos;
- 9.2.16.22. Detecção e resposta a ataques:
- 9.2.16.22.1. Monitorar continuamente os indicadores de possíveis ataque como *DCSync*, *DCShadow*, *Password Spraying*, *Password Guessing/Brute Force*, *Lsaas Injecton* nos controladores de domínio, *Golden Ticket*, *NTLM Relay*, entre outros;
 - 9.2.16.22.2. Detecção de ataques ao AD em tempo real ou em menos de um minuto;
 - 9.2.16.22.3. Análise detalhada do ataque, apresentando ativo de origem, vetor de ataque, controlador de domínio afetado, técnica aplicada;
 - 9.2.16.22.4. Apresentação de ataques em uma linha do tempo;
 - 9.2.16.22.5. Investigar ameaças, reproduzir ataques e procurar por *Backdoors*;
 - 9.2.16.22.6. Permitir busca ágil de eventos específicos na base da solução através de queries customizadas;
- 9.2.16.23. A solução deve ser capaz de enviar alertas por e-mail;
- 9.2.16.24. A solução nativamente deve ser capaz de se integrar com SIEM através de protocolo

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

SYSLOG;

- 9.2.16.25. A solução deve ser capaz de filtrar e enriquecer os eventos que serão enviados para o SIEM;
- 9.2.16.26. A solução deve produzir regras YARA na detecção de ataques (Ex. DCSync, Golden Ticket) identificados pela ferramenta;
- 9.2.16.27. A solução deve possuir conjunto de APIs REST, todas as chamadas disponíveis devem estar contidas na documentação;
- 9.2.16.28. A solução deve permitir a criação de listas de exclusões, suportando minimamente Exclusão por domínios do AD monitorados e por itens analisados;
- 9.2.16.29. A solução deve ser licenciada pelo número de usuários habilitados.

9.3. PROCESSO DE EXECUÇÃO DO SERVIÇO PARA GESTÃO DE VULNERABILIDADES

- 9.3.1. A fim de balizar todo o processo de gestão de vulnerabilidade da CONTRATANTE, e influenciado pelos principais *Frameworks* de boas práticas de serviços de segurança da informação, foi arquitetado o processo que será descrito nos parágrafos que seguem, o qual obrigatoriamente a CONTRATADA deve seguir *ipsis litteris*.
- 9.3.2. A CONTRATANTE deverá apresentar uma lista de ativos e recursos que deverão fazer parte do processo de gestão de vulnerabilidade. Tal lista poderá ser revisada e atualizada durante todo o período de vigência de contrato e deverá conter as seguintes informações mínimas, a saber:
- a) Nome do ativo e/ou serviço;
 - b) Grupo de serviço;
 - c) IP;
 - d) Janela de análise (Horário permitido para análise);
 - e) Prioridade.
- 9.3.3. A CONTRATADA deverá realizar de forma continuada uma avaliação prévia no ambiente computacional da CONTRATANTE a fim de consultivamente sugerir e complementar a lista de ativos e recursos que deverão fazer parte do processo de gestão de vulnerabilidade.
- 9.3.4. De acordo com as variáveis e critérios estabelecidos no catálogo de serviço e na lista de ativos e recursos da CONTRATANTE, a CONTRATADA deverá realizar checagens (*Scans*) e varreduras, buscando encontrar vulnerabilidades de segurança no ambiente da CONTRATANTE, utilizando as ferramentas e soluções definidas no presente termo de referência.
- 9.3.5. Após o término das rotinas de checagens (*Scans*) e varreduras no ambiente, deverá a CONTRATADA realizar uma análise de falso positivo das vulnerabilidades descobertas, isso

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

quer dizer, que devem ser informadas à CONTRATANTE apenas vulnerabilidades que existam de fato em seu ambiente.

- 9.3.6. Após análise de falso positivo, a CONTRATADA deverá informar ao CONTRATANTE as vulnerabilidades encontradas, obedecendo os critérios e requisitos estabelecidos no presente termo de referência.
- 9.3.7. Uma vez autorizada a mudança para correção de uma determinada vulnerabilidade, caberá a CONTRATADA sugerir as correções de vulnerabilidades encontradas no ambiente listado no tópico AMBIENTE TECNOLÓGICO DA CONTRATANTE (Hardware e Software), obrigatoriamente obedecendo as definições proposta pelo comitê de mudança da CONTRATANTE.
- 9.3.8. Para as vulnerabilidades encontradas no ambiente que ainda não tiverem soluções conhecidas, caberá à CONTRATADA apresentar medidas de contorno, que para aplicá-las ao ambiente, deverá obedecer ao ciclo de mudança estabelecido nos parágrafos anteriores.
- 9.3.9. Como último passo, a CONTRATADA deverá atualizar todos os controles e indicadores estabelecidos no presente termo de referência.
- 9.3.10. O processo descrito é o mínimo esperado a ser seguido e executado pela CONTRATADA. Todavia, como o objeto do presente termo de referência se trata de um serviço continuado, logo, se espera da CONTRATADA a apresentação de melhoria contínua deste, o qual pode ser alterado desde que aprovado pela CONTRATANTE.
- 9.3.11. O ciclo de vida do processo de gestão de vulnerabilidade deve ser executado de forma recorrente. A recorrência é definida em execuções de *Scans* quinzenais e apresentação dos resultados de forma mensal.

9.4. GRUPO TÉCNICO PARA EXECUÇÃO DO SERVIÇO

- 9.4.1. Através do seu Centro de Operações de Segurança definidos e especificados neste certame, a CONTRATADA deverá manter uma torre de operação denominada GRUPO DE ATAQUE CIBERNÉTICO CONTROLADO (Red Team), com objetivo e foco de trabalhar no processo de gestão de vulnerabilidade.
- 9.4.2. Estes profissionais deverão ser exclusivos para trabalhar no GRUPO DE ATAQUE CIBERNÉTICO (Red Team), não podendo os profissionais pertencentes a este grupo serem compartilhados e/ou atuarem com os demais serviços descritos no objeto do presente termo de referência.
- 9.4.3. Todos os profissionais que integram o grupo de ataque cibernético controlado devem obrigatoriamente compor o quadro permanente de colaboradores da CONTRATADA em regime de trabalho CLT (Consolidação das Leis do Trabalho) ou contrato de prestação de serviços firmados diretamente entre esses profissionais e a CONTRATADA, não havendo a possibilidade de terceirização ou subcontratação de tal serviço.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 9.4.4. Deverá ser de responsabilidade da CONTRATADA dimensionar o número adequado de profissionais para entrega de tal serviço sem que haja impacto no acordo de nível de serviço estabelecido no item Gestão de Vulnerabilidade do presente termo de referência.
- 9.4.5. A fim de garantir que os profissionais envolvidos tenham conhecimento e habilidade para executar o processo de gestão de vulnerabilidades no ambiente da CONTRATANTE, a CONTRATADA obrigatoriamente deverá compor o GRUPO DE ATAQUE CIBERNÉTICO CONTROLADO (*Red Team*) com ao menos 1 (um) perfil de cada que segue descrito abaixo:

Certificações	Descrição
- Linux LPIC 1, Linux LPIC 2 ou Linux LPIC 3 - CompTIA Security+ ou Certified Ethical Hacker	Diploma, devidamente registrado de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.

Tabela 4 - Certificações Grupo de Ataque Cibernético Controlado

- 9.4.6. Não existe restrição ou limite para acúmulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos no GRUPO DE ATAQUE CIBERNÉTICO CONTROLADO (*Red Team*), porém conforme já fora mencionado no presente termo de referência, este(s) deve(m) compor único e exclusivamente o time denominado GRUPO DE ATAQUE CIBERNÉTICO CONTROLADO (*Red Team*).
- 9.4.7. No momento da assinatura do contrato será exigido da CONTRATADA as seguintes documentações do(s) profissionais que participarão do GRUPO DE ATAQUE CIBERNÉTICO CONTROLADO (*Red Team*), os quais devem comprovar as exigências e obrigações descritas no presente termo de referência: contrato de prestação de serviços ou carteira de trabalho devidamente assinada pela CONTRATADA e as devidas certificações técnicas para comprovação do conhecimento.

9.5. ENTREGAS A SEREM REALIZADAS

- 9.5.1. Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, a CONTRATANTE definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue de forma *On Line* e em tempo de execução, através do portal de segurança descrito no tópico de condições gerais para prestação do serviço deste

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

termo de referência, a saber:

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Quantitativo de vulnerabilidades	Soma de vulnerabilidades	Vulnerabilidades	Vulnerabilidades	Número total de vulnerabilidades
Quantitativo de vulnerabilidades de severidade 5 por área responsável	Soma de vulnerabilidades de severidade 5 por área responsável	Vulnerabilidades de severidade 5	Vulnerabilidades	Número total de vulnerabilidades de severidade 5 por área responsável
Quantitativo de vulnerabilidades de severidade 4 por área responsável	Soma de vulnerabilidades de severidade 4 por área responsável	Vulnerabilidades de severidade 4	Vulnerabilidades	Número total de vulnerabilidades de severidade 4 por área responsável
Quantitativo de novas vulnerabilidades de severidades 4 e 5 por área responsável	Soma de novas vulnerabilidades de severidades 4 e 5 por área responsável	Vulnerabilidades de severidades 4 e 5	Vulnerabilidades	Número total de novas vulnerabilidades de severidades 4 e 5 por área responsável
Quantitativo de vulnerabilidades corrigidas de severidades 4 e 5 por área responsável	Soma de vulnerabilidades corrigidas de severidades 4 e 5 por área responsável	Vulnerabilidades corrigidas de severidades 4 e 5	Vulnerabilidades	Número total de vulnerabilidades corrigidas de severidades 4 e 5 por área responsável
Quantitativo de vulnerabilidades em Aplicações WEB	Soma de vulnerabilidades em Aplicações WEB	Vulnerabilidades em Aplicações WEB	Vulnerabilidades	Número total de vulnerabilidades em Aplicações WEB
Quantitativo de vulnerabilidades em Aplicações WEB de severidade 5	Soma de vulnerabilidades em Aplicações WEB de severidade 5	Vulnerabilidades em Aplicações WEB de severidade 5	Vulnerabilidades	Número total de vulnerabilidades em Aplicações WEB de severidade 5
Quantitativo de vulnerabilidades em Aplicações WEB de severidade 4	Soma de vulnerabilidades em Aplicações WEB de severidade 4	Vulnerabilidades em Aplicações WEB de severidade 4	Vulnerabilidades	Número total de vulnerabilidades em Aplicações WEB de severidade 4
Quantitativo de novas vulnerabilidades em Aplicações WEB de	Soma de novas vulnerabilidades em Aplicações WEB de	Vulnerabilidades em Aplicações WEB de	Vulnerabilidades	Número total de novas vulnerabilidades em aplicações WEB de severidades 4 e 5

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

WEB de severidades 4 e 5	severidades 4 e 5	severidades 4 e 5		
Quantitativo de vulnerabilidades corrigidas em Aplicações WEB de severidades 4 e 5	Soma de vulnerabilidades corrigidas em Aplicações WEB de severidades 4 e 5	Vulnerabilidades corrigidas em Aplicações WEB de severidades 4 e 5	Vulnerabilidades	Número total de vulnerabilidades corrigidas em Aplicações WEB de severidades 4 e 5
Quantitativo de certificados digitais expirados	Soma de certificados digitais expirados	Certificados digitais expirados	Certificados digitais	Número total de certificados digitais expirados
Quantitativo de certificados digitais a expirar em 3 meses	Soma de certificados digitais a expirar em 3 meses	Certificados digitais a expirar em 3 meses	Certificados digitais	Número total de certificados digitais a expirar em 3 meses
TOP 10 – Ativos mais vulneráveis	Soma de vulnerabilidades por ativo	Vulnerabilidades por ativo	Vulnerabilidades	TOP 10 do número de vulnerabilidades por ativo
TOP 10 – Vulnerabilidades mais comuns em ativos	Soma de vulnerabilidades	Vulnerabilidades	Vulnerabilidades	TOP 10 do número de vulnerabilidades
TOP 10 – Áreas responsáveis com maior número de vulnerabilidades	Soma de vulnerabilidades por área responsável	Vulnerabilidades por área responsável	Vulnerabilidades	TOP 10 do número de vulnerabilidades por área responsável
TOP 10 – Áreas responsáveis com maior número de vulnerabilidades de severidade 4 e 5	Soma de vulnerabilidades de severidade 4 e 5 por área responsável	Vulnerabilidades de severidade 4 e 5 por área responsável	Vulnerabilidades	TOP 10 do número de vulnerabilidades de severidade 4 e 5 por área responsável
TOP 10 – Áreas responsáveis com percentual de vulnerabilidades de severidade 4 e 5	Percentual de vulnerabilidades de severidade 4 e 5 por área responsável	Vulnerabilidades de severidade 4 e 5 por área responsável	Vulnerabilidades	TOP 10 do percentual de vulnerabilidades de severidade 4 e 5 por área responsável
TOP 10 – Aplicações WEB mais vulneráveis	Soma de vulnerabilidades	Vulnerabilidades em Aplicações WEB	Vulnerabilidades	TOP 10 do número total de

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

	em Aplicações WEB			vulnerabilidades em Aplicações WEB
TOP 10 – Aplicações WEB mais vulneráveis em comparação com OWASP	Soma de vulnerabilidades em Aplicações WEB em comparação com OWASP	Vulnerabilidades em Aplicações WEB	Vulnerabilidades	TOP 10 do número total de vulnerabilidades em Aplicações WEB em comparação com OWASP

Tabela 5 - Indicadores Estratégicos Gestão de Vulnerabilidade

10. MONITORAMENTO, DETECÇÃO E RESPOSTA A INCIDENTES PARA ENDPOINTS

- 10.1.1. A operação e gerenciamento de proteção avançada de *Endpoint* deverá seguir os preceitos técnicos definidos abaixo com o intuito da CONTRATADA ofertar plataforma de gestão avançada de segurança para *Endpoint*, agregando qualidade e mais proteção ao processo;
- 10.1.2. Cabe à CONTRATADA toda operação, dos níveis mais básicos (Nível 1) até o mais avançado (Nível 3).
- 10.1.3. Deverá ser criado usuário de leitura para equipe da CONTRATANTE, limitado à 4 profissionais de segurança da informação, para acompanhamento das ações na console de gerenciamento.
- 10.1.4. SOBRE A FERRAMENTA A SER UTILIZADA
 - 10.1.4.1. Realizar a pré-execução do agente para verificar o comportamento malicioso e detectar *Malware* desconhecido;
 - 10.1.4.2. O agente deve buscar algum sinal de *Malware* ativo e detectar *Malwares* desconhecidos;
 - 10.1.4.3. O agente deve ter a capacidade de submeter o arquivo desconhecido à nuvem de inteligência do fabricante para detectar a presença de ameaças;
 - 10.1.4.4. O agente deve realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes;
 - 10.1.4.5. A solução deve manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência;
 - 10.1.4.6. Deve realizar a verificação de todos os arquivos acessados em tempo real, mesmo durante o processo de *Boot*;
 - 10.1.4.7. Deve realizar a verificação de todos os arquivos no disco rígido em intervalos programados;
 - 10.1.4.8. Deve realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA);

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 10.1.4.9. Deve proteger os navegadores Internet Explorer, Firefox, Chrome, Opera, Safari e Microsoft Edge, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados;
- 10.1.4.10. Deve permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos;
- 10.1.4.11. É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, *Spyware*, *Trojans*, *Worms*, *Adware* e aplicativos potencialmente indesejados (PUAs);
- 10.1.4.12. Suportar equipamentos com arquitetura 32-bit e 64-bit que o cliente deve ter instalado nas estações de trabalho e deve ser compatível com os sistemas operacionais: Mac OS X 10.10, 10.11, 10.12, Microsoft Windows XP SP3, 7, e 10;
- 10.1.4.13. Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção;
- 10.1.4.14. Permitir a utilização de senha de proteção para permitir a reconfiguração local no cliente ou desinstalação dos componentes de proteção;
- 10.1.4.15. Funcionalidade de Firewall e Detecção e Proteção de Intrusão para estação com as funcionalidades:
- 10.1.4.16. Deve possuir atualização periódica de novas assinaturas de ataque;
- 10.1.4.17. Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (*Hash*) do arquivo;
- 10.1.4.18. Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas;
- 10.1.4.19. Possuir um sistema de prevenção de intrusão na estação (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados.
- 10.1.4.20. Deve aplicar uma análise adicional, inspecionando finalmente o comportamento de códigos durante a execução, para detectar comportamento suspeito de aplicações, tais como *Buffer Overflow*.
- 10.1.4.21. Deve possuir técnicas de proteção, que inclui:
- 10.1.4.22. Análise dinâmica de código - técnica para detectar *Malware* criptografado mais complexo;
- 10.1.4.23. Algoritmo correspondente padrão - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificados como um vírus;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

10.1.4.24. Possuir capacidade para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;

10.1.4.25. Possuir tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo. jpg.txt) ou a extensão não coincide com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt);

10.1.4.26. Verificação de ameaças web avançadas: bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise comportamental para identificar e parar o código malicioso de *Malware* avançado.

10.1.5. Funcionalidades de Antivírus e *Antispyware*

10.1.5.1. Proteção em tempo real contra vírus, *Trojans*, *Worms*, *Rootkits*, *Botnets*, *Spyware*, *Adwares* e outros tipos de códigos maliciosos.

10.1.5.2. Proteção *Anti-Malware* nativa da solução ou incorporada automaticamente por meio de *Plug-ins* sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante.

10.1.5.3. As configurações do *Anti-Spyware* deverão ser realizadas através da mesma console do antivírus;

10.1.5.4. Permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou *Malware*, permitir a inclusão de arquivos em listas de exclusão (*Whitelists*) para que não sejam verificados pelo produto;

10.1.5.5. Permitir a varredura das ameaças da maneira manual, agendada e em tempo real na máquina do usuário;

10.1.5.6. Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos, através do antivírus;

10.1.5.7. Capacidade de remoção automática total dos danos causados por *Spyware*, *Adwares* e *Worms*, como limpeza do registro e pontos de carregamento, com opção de finalizar o processo e terminar o serviço da ameaça no momento de detecção;

10.1.5.8. A remoção automática dos danos causados deve ser nativa do próprio antivírus; ou adicionada por plugin, desde que desenvolvido ou distribuído pelo fabricante;

10.1.5.9. Capacidade de bloquear origem de infecção através de compartilhamento de rede com opção de bloqueio da comunicação via rede;

10.1.5.10. Permitir o bloqueio da verificação de vírus em recursos mapeados da rede;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

10.1.5.11. Antivírus de Web (verificação de *Sites* e *Downloads* contra vírus);

10.1.6. Controle de Acesso a *Sites* por Categoria

10.1.6.1. Proteger a navegação na *Web*, mesmo aos usuários fora da rede, para todos os principais navegadores (IE, Firefox, Safari, Opera, Chrome e Microsoft Edge), fornecendo controle da *Internet* independentemente do *Browser* utilizado, como parte da solução de proteção a estações de trabalho, incluindo a análise do conteúdo baixado pelo navegador *Web*, de forma independente do navegador usado, ou seja, sem utilizar um *Plugin*, onde não é possível ser ignorada pelos usuários, protegendo os usuários de *Websites* infectados.

10.1.6.2. Funcionalidades específicas para prevenção contra a ação de *Ransomwares*, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos ou a capacidade de fazer *Backup* de arquivos antes de serem criptografados para posteriormente permitir sua restauração.

10.1.7. Funcionalidade de detecção Pró-Ativa de reconhecimento de novas ameaças.

10.1.7.1. Funcionalidade de detecção de ameaças via técnicas de *Deep Machine Learning*;

10.1.7.2. Funcionalidade de detecção de ameaças desconhecidas que estão em memória;

10.1.7.3. Capacidade de detecção, e bloqueio pró-ativo de *Keyloggers* e outros *Malwares* não conhecidos (ataques de dia zero) através da análise de comportamento de processos em memória (heurística);

10.1.7.4. Capacidade de detecção e bloqueio de *Trojans* e *Worms*, entre outros *Malwares*, por comportamento dos processos em memória;

10.1.7.5. Capacidade de analisar o comportamento de novos processos ao serem executados, em complemento à varredura agendada.

10.1.8. Funcionalidades de proteção contra *Ransomware*

10.1.8.1. Dispor de proteção contra *Ransomware* não baseada exclusivamente na detecção por assinaturas;

10.1.8.2. Dispor de remediação da ação de criptografia maliciosa dos *Ransomwares*;

10.1.8.3. A solução deve prevenir ameaças e interromper que eles sejam executados em dispositivos da rede, detectando e limpando os *Malwares*, além da realização de uma análise detalhada das alterações realizadas.

10.1.8.4. Possuir uma tecnologia *Anti-Exploit* baseada em comportamento, reconhecendo e bloqueando as mais comuns técnicas de *Malware*, protegendo os *Endpoints* de ameaças

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

desconhecidas e vulnerabilidades *Zero-Day*.

10.1.8.5. Deve ser realizada a detecção e o bloqueio de, pelo menos, as seguintes técnicas de exploit:

- a) DEP (Data Execution Prevention);
- b) Address Space Layout Randomization (ASLR);
- c) Bottom Up ASLR;
- d) Null Page;
- e) Anti-HeapSpraying;
- f) Dynamic Heap Spray;
- g) Import Address Table Filtering (IAF);
- h) VTable Hijacking;
- i) Stack Pivot and Stack Exec;
- j) SEHOP;
- k) Stack-based ROP (Return-Oriented Programming);
- l) Control-Flow Integrity (CFI);
- m) Syscall;
- n) WOW64;
- o) Load Library;
- p) Shellcode;
- q) VBScript God Mode;
- r) Application Lockdown;
- s) Process Protection;
- t) Network Lockdown;
- u) Remote reflective DLL injection;

10.1.8.6. *Local Privilege Escalation* – LPE.

10.1.8.7. A solução deve trabalhar silenciosamente na máquina do usuário e deve detectar a criptografia maliciosa de dados (*Ransomware*), realizando a sua interrupção. No caso de arquivos serem criptografados a solução deve realizar o retorno destes arquivos ao seu estado normal. Deste modo a solução deve fazer a limpeza e remoção completa do *Ransomware* na máquina do usuário.

10.1.8.8. Deve fornecer também uma análise detalhada das modificações realizadas pelo *Ransomware*, realizando a correlação dos dados em tempo real, indicando todas as

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

modificações feitas em registros, chaves, arquivos alvos, conexões de redes e demais componentes contaminados.

- 10.1.8.9. A console de monitoração e configuração deve ser feita através de uma central única, baseada em *Web* e em nuvem ou *Appliance* físico, que deve conter todas a ferramentas para a monitoração e controle da proteção dos dispositivos para a solução de *Anti-Exploit* e *Anti-Ransomware*.
- 10.1.8.10. A console deve apresentar painel com o resumo detalhado de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional, bem como todas as identificações para o mapeamento instantâneo dos efeitos causados pelo *Ransomware* nas estações de trabalho.
- 10.1.8.11. A solução deve implementar técnicas de EDR (*Endpoint Detection and Response*), possibilitando detecção e investigação nos *Endpoints* com atividades suspeitas;
- 10.1.8.12. Em caso de incidente a solução deve mostrar a trilha da infecção de forma visual, mostrando o início, todas as interações do *Malware* e o ponto final de bloqueio.
- 10.1.8.13. Após a análise da nuvem de inteligência do fabricante a solução deve apresentar um relatório sobre a ameaça contendo no mínimo:
- 10.1.8.14. Detalhes do Processo, como nome, *Hash*, hora e data da detecção e remediação;
- 10.1.8.15. Resultado da análise do arquivo suspeito pela funcionalidade de *Machinne Learning* ou *Deep Learning*;
- 10.1.8.16. Propriedades gerais do arquivo, como nome, versão, tamanho, idioma, informações de certificado;
- 10.1.8.17. A solução de EDR deve ser integrada ao agente de antivírus, instalada como um agente único em estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;
- 10.1.8.18. O gerenciamento da solução de EDR deve ser feito a partir da mesma Console de Gerenciamento da solução antivírus;
- 10.1.8.19. Deve fornecer guias de respostas a incidentes, fornecendo visibilidade sobre o escopo de um ataque, como ele começou, o que foi impactado, e como responder;
- 10.1.8.20. Deve responder ao incidente com opção de isolamento da máquina, bloqueio e limpeza da ameaça;
- 10.1.8.21. Deve realizar buscas de ameaças em todo o ambiente, permitir buscar por *Hash*, nome, endereços IP, domínio ou linha de comando;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 10.1.8.22. Funcionalidade de Controle de Aplicações e Dispositivos Externos:
- 10.1.8.23. Possuir controle de aplicativos para monitorar e impedir que os usuários executem ou instalem aplicações que podem afetar a produtividade ou o desempenho da rede;
- 10.1.8.24. Atualizar automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicativos específicos ou categorias específicas de aplicações possam ser liberadas ou bloqueadas;
- 10.1.8.25. Verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões. Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web;
- 10.1.8.26. Oferecer proteção para chaves de registro e controle de processos;
- 10.1.8.27. Proibir através de política a inicialização de um processo ou aplicativo com base no nome e no *Hash* do arquivo;
- 10.1.8.28. Detectar um aplicativo controlado quando os usuários o acessarem, com as opções de permitir e alertar ou bloquear e alertar;
- 10.1.8.29. Possuir a opção de customizar uma mensagem a ser mostrada ao usuário em caso de bloqueio de execução do aplicativo;
- 10.1.8.30. Gerenciar o uso de dispositivos de armazenamento USB (ex: pen-drives e HDs USB). Permitir, através de regras, o bloqueio ou liberação da leitura/escrita/execução do conteúdo desses dispositivos;
- 10.1.8.31. Controlar o uso de outros dispositivos periféricos, como comunicação infravermelha e modem externo;
- 10.1.8.32. As funcionalidades do Controle de Aplicações e Dispositivos deverão ser nativas do produto ou incorporadas automaticamente por meio de *Plugins* sem utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante;
- 10.1.8.33. Controle de vulnerabilidades do Windows e dos aplicativos instalados:
- 10.1.8.34. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
- 10.1.8.35. A gestão desses dispositivos deve ser feita diretamente na Console de Gerenciamento, deve permitir definir políticas diferentes por grupos de *Endpoints*;
- 10.1.8.36. Permitir a autorização de um dispositivo com no mínimo as seguintes opções:
- Permitir que todos os dispositivos do mesmo modelo;
 - Permitir que um único dispositivo com base em seu número de identificação único;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- c) Permitir o acesso total;
- d) Permitir acesso somente leitura.

10.1.9. Funcionalidades Contra-Ataques Avançados, Detecção e Resposta.

- 10.1.9.1. A solução deve ter capacidade de implementar técnicas avançada contra-ataque, detecção e resposta, possibilitando detecção e investigação nas estações de trabalho com atividades suspeitas;
- 10.1.9.2. Em caso de incidente a solução deve mostrar a trilha da infecção de forma visual, mostrando o início, todas as interações do *Malware* e o ponto final de bloqueio.
- 10.1.9.3. Após a análise da nuvem de inteligência do fabricante a solução deve apresentar um relatório sobre a ameaça contendo no mínimo:
- 10.1.9.4. Detalhes do Processo, como nome, *Hash*, hora e data da detecção e remediação;
- 10.1.9.5. Reputação do arquivo e correlação da detecção do arquivo em outras soluções de antivírus através de bases de conhecimento como o Vírus Total ou do próprio fabricante;
- 10.1.9.6. Resultado da análise do arquivo suspeito pela funcionalidade de *Machinne Learning* ou *Deep Learning*;
- 10.1.9.7. Propriedades gerais do arquivo, como nome, versão, tamanho, idioma, informações de certificado;
- 10.1.9.8. A solução de EDR (*Endpoint Detection and Response*) deve ser integrada ao agente de antivírus, instalada como um agente único em estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;
- 10.1.9.9. O gerenciamento da solução de EDR deve ser feito a partir da mesma console de gerenciamento da solução antivírus;
- 10.1.9.10. Deve fornecer guias de respostas a incidentes, fornecendo visibilidade sobre o escopo de um ataque, como ele começou, o que foi impactado, e como responder;
- 10.1.9.11. Deve responder ao incidente com opção de isolamento da máquina, bloqueio e limpeza da ameaça;
- 10.1.9.12. Deve realizar buscas de ameaças em todo o ambiente, permitir buscar por *Hash*, nome, endereços IP, domínio ou linha de comando;
- 10.1.10. Funcionalidade de Controle de Aplicações e Dispositivos:
 - 10.1.10.1. Oferecer proteção para chaves de registro e controle de processos;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 10.1.10.2. Proibir, através de política a inicialização de um processo ou aplicativo, com base no nome e no *Hash* do arquivo;
- 10.1.10.3. Gerenciar o uso de dispositivos de armazenamento USB (ex: pen-drives e HDs USB). Permitir, através de regras, o bloqueio ou liberação da leitura/escrita/execução do conteúdo desses dispositivos;
- 10.1.10.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
- 10.1.10.5. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
- 10.1.10.6. A gestão desses dispositivos deve ser feita diretamente na console de gerenciamento e permitir definir políticas diferentes por grupos de *Endpoints*;
- 10.1.10.7. Permitir a autorização de um dispositivo com no mínimo as seguintes opções:
- a) Permitir todos os dispositivos do mesmo modelo;
 - b) Permitir um único dispositivo com base em seu número de identificação único;
 - c) Permitir o acesso total;
 - d) Permitir acesso somente leitura.
- 10.1.10.8. Proteger servidores contra *Malwares*, arquivos e tráfego de rede malicioso, controle de periféricos, controle de acesso à web, controle de aplicativos em um único agente instalado nos servidores;
- 10.1.10.9. Realizar a pré-execução do agente para verificar o comportamento malicioso e detectar *Malwares* desconhecidos;
- 10.1.10.10. O agente *Host* deve buscar algum sinal de *Malwares* ativos e detectar *Malwares* desconhecidos;
- 10.1.10.11. O agente deve realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes;
- 10.1.10.12. A solução deve manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência;
- 10.1.10.13. Realizar a verificação de todos os arquivos acessados em tempo real, mesmo durante o processo de *Boot*;
- 10.1.10.14. Realizar a verificação de todos os arquivos no disco rígido em intervalos programados;
- 10.1.10.15. Realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

e aplicações potencialmente indesejáveis (PUA);

- 10.1.10.16. Proteger os navegadores Internet Explorer, Firefox, Chrome, Opera, Safari e Microsoft Edge, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados;
- 10.1.10.17. Permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos;
- 10.1.10.18. É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, *Spyware*, *Trojans*, *Worms*, *Adware* e aplicativos potencialmente indesejados (PUAs);
- 10.1.10.19. O cliente para instalação em servidores deve ser compatível com os sistemas operacionais abaixo:
 - a) Windows Server 2022;
 - b) Windows Server 2019;
 - c) Windows Server 2016;
 - d) Windows Server 2012 R2 (64 bit);
 - e) Windows Server 2012 (64 bit);
 - f) Windows Server 2008 R2 (64 bit);
 - g) Ubuntu (versão atual 20.04 ou superior).
- 10.1.10.20. Suportar a inclusão de outros servidores para a função de atualização distribuída e cache, de forma a agilizar o processo de atualização dos demais agentes;
- 10.1.10.21. Possuir integração com as nuvens da Microsoft Azure e Amazon Web Services para identificar as informações dos servidores instanciados nas nuvens;
- 10.1.10.22. Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção;
- 10.1.10.23. Permitir a utilização de senha de proteção para permitir a reconfiguração local no cliente ou desinstalação dos componentes de proteção;
- 10.1.10.24. Funcionalidade de *Firewall* e Detecção e Proteção de Intrusão (IDS/IPS);
- 10.1.10.25. Possuir proteção contra exploração de *Buffer Overflow*;
- 10.1.10.26. Possuir proteção contra-ataques de Negação de Serviço (Denial of Service - DoS), Port-Scan, MAC Spoofing e IP Spoofing;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 10.1.10.27. Possuir atualização periódica de novas assinaturas de ataque;
- 10.1.10.28. Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (*Hash*) do arquivo.
- 10.1.10.29. Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas;
- 10.1.10.30. Possuir um sistema de prevenção de intrusão no *Host* (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados.
- 10.1.10.31. Identificar comportamentos suspeitos de códigos e ataques de dia zero (*Zero Day*), tais como: *Buffer Overflow*, tráfego de códigos maliciosos e atividades suspeitas detectadas por comportamento.
- 10.1.10.32. Possuir técnicas de proteção, que inclui:
- Análise dinâmica de código - técnica para detectar *Malware* criptografado mais complexo;
 - Algoritmo correspondente padrão - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificado como um vírus;
 - Possuir capacidade para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;
 - Possuir tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo. jpg.txt) ou a extensão não coincida com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt);
 - Verificação de ameaças *Web* avançadas: bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise comportamental para identificar e parar o código malicioso de *Malware* avançados.
- 10.1.11. Funcionalidade de Antivírus e *AntiSpyware*:
- 10.1.11.1. Proteção em tempo real contra vírus, *Trojans*, *Worms*, *Rootkits*, *Botnets*, *Spyware*, *Adwares* e outros tipos de códigos maliciosos.
- 10.1.11.2. Proteção *Anti-Malware* nativa da solução ou incorporada automaticamente por meio de *Plug-Ins* sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante.
- 10.1.11.3. As configurações do *Anti-Spyware* devem ser realizadas através da mesma console do

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

antivírus;

- 10.1.11.4. Permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou *Malware*, permitir a inclusão de arquivos em listas de exclusão (*Whitelists*) para que não sejam verificados pelo produto;
- 10.1.11.5. Permitir a varredura das ameaças da maneira manual, agendada e em tempo real nos servidores;
- 10.1.11.6. Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do antivírus;
- 10.1.11.7. Capacidade de detectar arquivos através da reputação dos mesmos;
- 10.1.11.8. Capacidade de remoção automática total dos danos causados por *Spyware*, *Adwares* e *Worms*, como limpeza do registro e pontos de carregamento, com opção de finalizar o processo e terminar o serviço da ameaça no momento de detecção;
- 10.1.11.9. A remoção automática dos danos causados deve ser nativa do próprio antivírus; ou adicionada por *Plugin*, desde que desenvolvido ou distribuído pelo fabricante;
- 10.1.11.10. Bloquear origem de infecção através de compartilhamento de rede com opção de bloqueio da comunicação via rede;
- 10.1.11.11. Detectar tráfego de rede para comandar e controlar os servidores;
- 10.1.11.12. Proteger arquivos de documento contra-ataque do tipo *Ransomwares*;
- 10.1.11.13. Proteger contra ataques de *Ransomware* em pastas compartilhadas na rede;
- 10.1.11.14. Permitir o envio de amostras de *Malwares* para a nuvem de inteligência do fabricante;
- 10.1.11.15. Permitir o bloqueio da verificação de vírus em recursos mapeados da rede;
- 10.1.11.16. Antivírus de *Web* (verificação de *Sites* e *Downloads* contra vírus).
- 10.1.12. Gerenciamento e administração centralizada
 - 10.1.12.1. A console de monitoração e configuração deve ser feita através de uma central para o grupo de *Anti-Malware*, baseada em *Web* e em nuvem ou *Appliance*, que deve conter todas as ferramentas para a monitoração e controle da proteção dos dispositivos;
 - 10.1.12.2. A console deve apresentar painel com o resumo dos *Status* de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 10.1.12.3. Possuir mecanismo de comunicação via API, Syslog ou RESTFULL API (*Representational State Transfer*), para integração com outras soluções de segurança, disponibilizando acesso a documentação técnica da API do fabricante;
- 10.1.12.4. A console deve permitir a divisão dos computadores, dentro da estrutura de gerenciamento em grupos;
- 10.1.12.5. Permitir sincronização com o *Active Directory* (AD) para gestão de usuários e grupos integrados às políticas de proteção.
- 10.1.12.6. Aplicar regras diferenciadas baseado em grupos ou usuários;
- 10.1.12.7. A instalação deve ser feita via cliente específico por *Download* da gerência central ou também via *Email* de configuração. O instalador deve permitir a distribuição do cliente via *Active Directory* (AD) para múltiplas máquinas;
- 10.1.12.8. A console deve permitir criar e editar diferentes políticas para a aplicação das proteções exigidas e aplicadas a nível de usuários ou *Endpoint*, não importando em que equipamentos eles estejam acessando;
- 10.1.12.9. Fornecer atualizações do produto e das definições de vírus e proteção contra intrusos;
- 10.1.12.10. Permitir exclusões de escaneamento para um determinado *Website*, pasta, arquivo ou aplicação, tanto a nível geral quanto específico em uma determinada política.
- 10.1.12.11. A console de gerenciamento deve permitir a definição de grupos de usuários com diferentes níveis de acesso as configurações, políticas e *Logs*;
- 10.1.12.12. Atualização incremental, remota e em tempo-real, da vacina dos antivírus e do mecanismo de verificação (*Engine*) dos clientes;
- 10.1.12.13. Permitir o agendamento da varredura contra vírus, permitir selecionar uma máquina, grupo de máquinas ou domínio, com periodicidade definida pelo administrador;
- 10.1.12.14. Atualização automática das assinaturas de ameaças (*Malwares*) e políticas de prevenção desenvolvidas pelo fabricante em tempo real ou com periodicidade definida pelo administrador;
- 10.1.12.15. Utilizar protocolos seguros padrão HTTPS para comunicação entre console de gerenciamento e clientes gerenciados.
- 10.1.12.16. As mensagens geradas pelo agente devem estar no idioma em português ou permitir a sua edição.
- 10.1.12.17. Recursos do relatório e monitoramento devem ser nativos da própria console central de gerenciamento;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 10.1.12.18. Exibir informações como nome da máquina, versão do antivírus, sistema operacional, versão da *Engine*, data da vacina, data da última verificação, eventos recentes e *Status*;
- 10.1.12.19. Capacidade de geração de relatórios, estatísticos ou gráficos, tais como:
- 10.1.12.20. Detalhar quais usuários estão ativos, inativos ou desprotegidos, bem como detalhes dos mesmos;
- 10.1.12.21. Detalhamento dos computadores que estão ativos, inativos ou desprotegidos, bem como detalhes das varreduras e dos alertas nos computadores;
- 10.1.12.22. Detalhamento dos periféricos permitidos ou bloqueados, bem como detalhes de onde e quando cada periférico foi usado;
- 10.1.12.23. Detalhamento das principais aplicações bloqueadas e os servidores/usuários que tentaram acessá-las;
- 10.1.12.24. Detalhamento das aplicações permitidas que foram acessadas com maior frequência e os servidores/usuários que as acessam;
- 10.1.12.25. Detalhamento dos servidores/usuários que tentaram acessar aplicações bloqueadas com maior frequência e as aplicações que eles tentaram acessar;
- 10.1.12.26. Detalhamento de todas as atividades disparadas por regras de prevenção de perda de dados.
- 10.1.12.27. Possuir um elemento de comunicação para mensagens e notificações entre estações e a console de gerenciamento utilizando comunicação criptografada;
- 10.1.12.28. Fornecer solução de gerenciamento de arquivos armazenados em nuvem, garantindo que um arquivo que foi feito um *Upload* (exemplo Dropbox, Google Drive, OneDrive), tenha o processo monitorado e gerenciado, bem como realizar automaticamente o escaneamento do arquivo contra *Malwares*, procuradas palavras chaves ou informações confidenciais. Deve ser bloqueado o *Upload* ou removida a informação confidencial antes do envio do arquivo;
- 10.1.12.29. As portas de comunicação deverão ser configuráveis. A comunicação deve permitir QoS para controlar a largura de banda de rede.
- 10.1.12.30. A solução deve permitir a seleção da versão do *Software* de preferência, permitindo assim o teste da atualização sobre um grupo de PCs piloto antes de implantá-lo para toda a rede. Permitir ainda selecionar um grupo de computadores para aplicar a atualização para controlar a largura de banda de rede. A atualização da versão deve ser transparente para os usuários finais.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 10.1.12.31. O agente antivírus deve proteger *Laptops*, *Desktops* e servidores em tempo real, sob demanda ou agendado para detectar, bloquear e limpar todos os vírus, *Trojans*, *Worms* e *Spyware*. No Windows o agente também deve detectar PUA, *Adware*, comportamento suspeito, controle de aplicações e dados sensíveis. O agente ainda deve fornecer controle de dispositivos terceiros e, controle de acesso à web;
- 10.1.12.32. Possuir mecanismo contra a desinstalação do *Endpoint* pelo usuário e cada dispositivo deve ter uma senha única;
- 10.1.12.33. Prover no *Endpoint* a solução de HIPS (*Host Intrusion Prevention System*) para a detecção automática e proteção contra comportamentos maliciosos (análise de comportamento) e deve ser atualizado diariamente;
- 10.1.12.34. Prover proteção automática contra *Web Sites* infectados e maliciosos, assim como prevenir o ataque de vulnerabilidades de *Browser* via *Web Exploits*;
- 10.1.12.35. Permitir a monitoração e o controle de dispositivos removíveis nos equipamentos dos usuários, como dispositivos USB, periféricos da própria estação de trabalho e redes sem fio;
- 10.1.12.36. O controle de dispositivos deve ser ao nível de permissão, somente leitura ou bloqueio;
- 10.1.12.37. A ferramenta de administração centralizada deve gerenciar todos os componentes da proteção para estações de trabalho e servidores e deve ser projetada para a fácil administração, supervisão e elaboração de relatórios dos *Endpoint* e servidores;
- 10.1.12.38. Possuir interface gráfica *Web*, com suporte a língua portuguesa (padrão brasileiro);
- 10.1.12.39. A Console de administração deve incluir um painel com um resumo visual em tempo real para verificação do *Status* de segurança;
- 10.1.12.40. Fornecer filtros pré-construídos que permitam visualizar e corrigir apenas os computadores que precisam de atenção;
- 10.1.12.41. Exibir os PCs gerenciados de acordo com critérios da categoria (detalhes do estado do computador, detalhes sobre a atualização, detalhes de avisos e erros, detalhes do antivírus etc.), e classificar os PCs em conformidade;
- 10.1.12.42. Uma vez que um problema seja identificado, permitir corrigir os problemas remotamente, com no mínimo as opções abaixo:
- Proteger o dispositivo com a opção de início de uma varredura;
 - Forçar uma atualização naquele momento;
 - Ver os detalhes dos eventos ocorridos;
 - Executar verificação completa do sistema;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- e) Forçar o cumprimento de uma nova política de segurança;
- f) Mover o computador para outro grupo;
- g) Apagar o computador da lista.

10.1.12.43. Atualizar a políticas de segurança quando um computador for movido de um grupo para outro manualmente ou automaticamente;

10.1.12.44. Permitir exportar o relatório de *Logs* de auditoria nos formatos CSV e PDF;

10.1.12.45. Deve conter vários relatórios para análise e controle dos usuários e *Endpoints*. Os relatórios deverão ser divididos, no mínimo, em relatórios de: eventos, usuários, controle de aplicativos, periféricos e *Web*, indicando todas as funções solicitadas para os *Endpoints*;

10.1.12.46. Fornecer relatórios utilizando listas ou gráficos, utilizando informações presentes na console, com no mínimo os seguintes tipos:

- a) Nome do dispositivo;
- b) Início da proteção;
- c) Último usuário logado no dispositivo;
- d) Último *Update*;
- e) Último escaneamento realizado;
- f) *Status* de proteção do dispositivo;
- g) Grupo a qual o dispositivo faz parte;

10.1.12.47. Permitir a execução manual de todos estes relatórios nos formatos CSV e PDF;

10.2. PROCESSO DE EXECUÇÃO DO SERVIÇO MONITORAMENTO, DETECÇÃO E RESPOSTA A INCIDENTES PARA ENDPOINTS

10.2.1. O gerenciamento da solução de segurança Endpoint Security deverá contemplar as atividades listadas abaixo.

10.2.1.1. Administração da solução de Endpoint Security seguindo as melhores práticas do fabricante da solução;

10.2.1.2. Configuração da console de gerência;

10.2.1.3. Realizar health check mensal na plataforma para otimizar configurações de forma corretiva ou preventiva visando a redução de riscos de segurança e elevação do nível de maturidade;

10.2.1.4. Instalar, configurar e documentar novos componentes ou novas funcionalidades que

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

estiverem disponíveis no produto;

- 10.2.1.5. Customizar relatórios nativos a partir da solução de gerência da solução de Endpoint Security;
- 10.2.1.6. Instalação remota dos agentes nos dispositivos (servidores e desktops e notebooks).
- 10.2.1.7. Identificar e corrigir de forma proativa ou corretiva problemas na eficácia do endpoint gerenciado;
- 10.2.1.8. Integrar a solução com o ambiente do cliente utilizando integrações nativas que não dependam de desenvolvimento, como por exemplo, autenticação LDAP, envio de alertas de e-mails via relay;
- 10.2.1.9. Configurar alertas e notificações na plataforma, conforme alinhamento com o cliente;
- 10.2.1.10. Corrigir falhas e problemas que impactem nas funcionalidades ou disponibilidade da aplicação que não dependam diretamente da infraestrutura local como acesso à internet, falhas de comunicação decorrentes de falhas de rede, falhas no sistema de virtualização etc.;
- 10.2.1.11. Notificar o cliente sempre que houver novas versões do produto, elaborar documento de implantação para execução do upgrade e realizar upgrade da solução após aprovação formal do cliente;
- 10.2.1.12. Apoiar na criação das rotinas de backup e restore da solução em casos de desastres seguindo as recomendações e melhores práticas do fabricante da solução;
- 10.2.1.13. Em casos de incidentes de segurança que impactem o funcionamento da solução de Endpoint Security a CONTRATADA deverá apoiar na reconstrução do ambiente administrado por este contrato;
- 10.2.1.14. Atender a requisições de serviço que tratem de dúvidas sobre funcionalidade ou configurações do produto adquirido neste contrato;
- 10.2.1.15. Realizar reuniões mensais para acompanhamento dos resultados;
- 10.2.1.16. Acionar equipe de Segurança da Informação da CONTRATANTE para auxiliar em diagnóstico e tratamento de problemas de maior complexidade e impacto;
- 10.2.1.17. Certificar diariamente que as atualizações de vacinas estejam sendo recebidas e distribuídas para o parque de ativos;
- 10.2.1.18. Definir e manter atualizado os procedimentos operacionais relacionados a solução listados abaixo.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 10.2.1.18.1. Troubleshooting de comunicação.
- 10.2.1.18.2. Troubleshooting de vacinas.
- 10.2.1.18.3. Troubleshooting de funcionamento do agente.
- 10.2.1.18.4. Procedimento de instalação do agent.
- 10.2.1.18.5. Tratamento de incidentes relacionados a solução de Endpoint Security.

10.2.2. ENTREGAS A SEREM REALIZADAS

10.2.2.1. Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, o CONTRATANTE definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue de forma on line e em tempo de execução, através do portal de indicadores descrito no tópico de condições gerais para prestação do serviço deste termo de referência, a saber:

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Ameaças identificadas na solução de endpoint Security	Soma de ameaças	Ameaças	Ameaças	Número total de Ameaças
Conformidade de assinaturas nos endpoints gerenciados	Soma de não conformidade	Tipos com maior frequência	Conformidade	Número total de não conformidade por tipo
Cobertura de proteção dos endpoints descoberto vs instalado	Soma de divergência	Protegido	Protegidos	% do parque protegido

Tabela 6 - Indicadores Estratégicos de Monitoramento de EndPoints

11. DO PAGAMENTO DOS SERVIÇOS

- 11.1. A prestação dos serviços será baseada no modelo de remuneração em função dos resultados apresentados, em que os pagamentos serão feitos após mensuração do Nível Mínimo de Serviço (NMS) definido em contrato/Termo de Referência, de modo a resguardar a eficiência e a qualidade na prestação dos serviços.
- 11.2. Os pagamentos terão início somente após a instalação da solução e a completa disponibilização dos serviços, mediante o aceite definitivo da CONTRATANTE.
 - 11.2.1. O CRCMG efetuará o pagamento em até 10 (dez) dias úteis, contados a partir do recebimento da Nota Fiscal com as devidas deduções legais.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 11.2.2. Considera-se ocorrido o recebimento da nota fiscal ou fatura no momento em que o CRCMG contratante atestar a execução do objeto do contrato.
- 11.2.3. A Nota Fiscal deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da Lei nº 8.666, de 1993.
- 11.3. Serão descontados sobre o pagamento a ser realizado, as devidas retenções de tributos e contribuições, conforme determina a Instrução Normativa nº. 1.234, de 11/01/2012, da Secretaria da Receita Federal.
- 11.4. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para o CRCMG.
- 11.5. Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.
- 11.6. Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do CRCMG.
- 11.7. Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018.
- 11.8. Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.
- 11.9. Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.
- 11.10. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.
- 11.11. Será rescindido o contrato em execução com a contratada inadimplente no SICAF, salvo por motivo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 11.12. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

$EM = I \times N \times VP$, sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

$$I = (TX) \quad I = \frac{(6 / 100)}{365} \quad TX = \text{Percentual da taxa anual} = 6\% \\ I = 0,00016438$$

- 11.13. Os preços são fixos e irreajustáveis no prazo de um ano contado da data limite para a apresentação das propostas.

- 11.14. Dentro do prazo de vigência do contrato e mediante solicitação da contratada, os preços contratados poderão sofrer reajuste após o interregno de um ano, aplicando-se o índice IPCA acumulado nos 12 (doze) meses anteriores a data base ou outro índice que venha a substituí-lo, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

- 11.15. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

12. DA MENSURAÇÃO

- 12.1. O pagamento será feito mensalmente, levando-se em consideração o Nível Mínimo de Serviço (NMS) acordado em contrato, para o período de faturamento avaliado. O valor a ser pago será o valor unitário do item correspondente, alinhado com o NMS previsto em contrato.

- 12.2. Conforme ACORDO DE NÍVEIS DE SERVIÇO os SERVIÇOS GERENCIADOS DE SEGURANÇA serão medidos, nos seguintes termos:

- 12.2.1. DISPONIBILIDADE MENSAL DOS GRUPOS DE TECNOLOGIAS: Acompanha a execução do SERVIÇO DE GESTÃO DE DISPONIBILIDADE sobre os ativos de segurança, sob responsabilidade da CONTRATADA.

- 12.2.2. As qualificações técnicas exigidas para o perfil de analista(s) que participará do supracitado GRUPO DE DISPONIBILIDADE, da CONTRATADA:

Perfis	Certificações	Descrição
Analista de Segurança I	ITIL foundation V3 Ou	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

	ISFS (Information Security Foundation)	da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento pleno em segurança da informação, realizando monitoramento de disponibilidade de ambiente de segurança da informação, similares ao ambiente supracitado. Experiência comprovada de no mínimo 12 (doze) meses em tecnologia da informação.

Tabela 7 – Qualificações Grupo de Disponibilidade

12.2.3. No momento da assinatura do contrato, será exigido da CONTRATADA, a apresentação das documentações do(s) profissionais que participarão do GRUPO DE DISPONIBILIDADE, as quais devem comprovar as exigências e obrigações descritas neste termo de referência: contrato de prestação de serviços ou carteira de trabalho devidamente assinada pela CONTRATADA, para comprovação de habilidades, e as devidas certificações técnicas para comprovação do conhecimento conforme TABELA de exigências de qualificações.

12.2.4. ENTREGA MENSAL DOS SERVIÇOS:

12.2.4.1. Acompanha a execução de todos os demais serviços que compõem o objeto SERVIÇOS GERENCIADOS DE SEGURANÇA, sobre os ativos de segurança sob responsabilidade da CONTRATADA.

TIPO DE PRIORIDADE	QUANTIDADE DE ATENDIMENTO REALIZADO NO PERÍODO	QUANTIDADE DE ATENDIMENTO DESACORDO COM O NMS	FATOR DE ABATIMENTO POR DESEMPENHO DE SERVIÇO
P1			
P2			
P3			
P4			
P5			
P6			
P7			
P8			
VTAD (Valor R\$ total apurado)			

Tabela 8 – Dashboard de entrega de serviços

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR
Tipo de prioridade	N/A	N/A	N/A

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

Quantidade de atendimento realizado no período	Soma de todos os atendimentos realizados no período	Período de apuração	Prioridade
Quantidade de atendimento desacordo com o NMS	Soma de todos os atendimentos realizados no período que não estão em conformidade com o NMS supracitado	Período de apuração	Prioridade
Fator de abatimento por desempenho de serviço (FADS)	Conforme item ENTREGA MENSAL DOS SERVIÇOS GERENCIADOS DE SEGURANÇA	Período de apuração	Prioridade
VTAD (Valor R\$ total apurado)	Soma do total de FADS, e subtrai do valor total previsto para o período	Período de apuração	N/A

Tabela 9 – Legenda de entrega de serviços

- 12.3. A reunião mensal deverá ocorrer até o 5º (quinto) dia útil após o término do período de faturamento, que coincidirá com o mês legal, e a disponibilidade dos relatórios será condição necessária ao recebimento dos serviços pelo CONTRATANTE. O primeiro mês de faturamento será parcial e proporcional, contado da data da emissão do termo de recebimento definitivo até o último dia do mês. Neste contexto, o profissional deve apresentá-lo de forma virtual, por meio de solução de videoconferência.
- 12.4. A respectiva nota fiscal/fatura, já deduzidos os fatores de abatimento calculados, deverá ser emitida somente após o recebimento definitivo dos serviços, e após a homologação das informações apresentadas pela CONTRATADA ao CONTRATANTE.
- 12.5. Caso não haja concordância da CONTRATADA com os fatores de abatimento calculados, os mesmos serão convertidos em sanção, aplicação de multa de mesmo valor, de forma a garantir o contraditório e a ampla defesa.
- 12.6. A qualquer tempo e a critério do CONTRATANTE, a bases dos sistemas utilizados para cálculo das entregas e indicadores listados neste tópico poderão ser solicitadas para auditorias e aferições.

13. DA ABRANGÊNCIA E ESCOPO DOS SERVIÇOS:

- 13.1. Considerar-se-á, para efeitos desta contratação, todos os recursos necessários para a perfeita execução efetiva da prestação dos serviços.
- 13.2. O dimensionamento da equipe para a execução adequada do serviço contratado é de responsabilidade exclusiva da CONTRATADA, devendo ser suficiente para o cumprimento integral dos níveis de serviço exigidos neste Termo de Referência.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

13.3. Dependendo da complexidade, criticidade e do prazo do projeto, os serviços poderão ser realizados nas instalações da CONTRATADA ou da CONTRATANTE.

13.4. Todos os custos com licenças de simuladores, *Softwares* devem estar contabilizados no valor do serviço, não sendo permitido o pagamento de valores adicionais ou extras, seja a que título for.

14. EXECUÇÃO DOS SERVIÇOS

14.1. A contratada deverá cumprir o seguinte cronograma de implantação dos serviços:

CRONOGRAMA DE IMPLANTAÇÃO		
ITENS	SERVIÇOS PREVISTOS:	PRAZO
1	Reunião de início de projeto (Kick-Off). Deverá ser previamente agendada pela CONTRATADA com até 02 (dois) dias úteis de antecedência.	10*
2	Entrega do Projeto Executivo pela CONTRATADA , a partir da reunião de início do projeto (Kick-Off).	30*
3	Manifestação de reajustes pela CONTRATANTE , se for o caso, a partir da data de entrega do Projeto Executivo.	10*
4	Ajustes, se for o caso, no Projeto Executivo pela CONTRATADA , a partir da manifestação de reajustes pela CONTRATANTE .	10*
5	Centro de Operações de Segurança da CONTRATADA em pleno funcionamento e operação em regime 24x7x365, a partir da data de início da vigência do contrato.	75*
6	Conclusão da fase de implantação dos serviços, contados a partir da data de início da vigência do contrato. Após a emissão do termo de recebimento definitivo pela CONTRATANTE .	90*
7	Disponibilidade dos serviços pela CONTRATADA .	60 meses**

Tabela 10 – Cronograma de implantação

* Prazos em dias corridos contados da data de assinatura do contrato.

** Prazo em meses contado a partir da assinatura do contrato.

14.2. A CONTRATADA deverá atender às seguintes condições gerais para início da prestação de cada um dos serviços, incluindo fase de concepção da solução, confecção de Projeto Executivo, planejamento de atividades de instalação, customização de ambiente e ativação de serviços sem ônus adicionais ao CONTRATANTE:

14.2.1. Reunião de início do projeto (*Kick-Off*), a ser realizada em até 10 (dez) dias corridos após a assinatura do contrato, a ser previamente agendada pela CONTRATADA com 02 (dois) dias úteis de antecedência.

14.2.1.1. A reunião deverá ser realizada preferencialmente de forma remota.

14.2.2. Serão de responsabilidade da CONTRATADA as atividades de instalação, integração,

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

configuração e testes de todos os produtos componentes de cada solução alocada, excluindo-se a Solução de Segurança da CONTRATANTE já ativa (Firewall), em conformidade com o Projeto Executivo a ser elaborado e apresentado pela CONTRATADA para prévia aprovação pela CONTRATANTE;

- 14.2.3. A CONTRATADA deverá levantar informações acerca dos locais de instalação dos produtos durante a elaboração do Projeto Executivo, e, se necessário, efetuar visita técnica para verificar eventuais requisitos físicos a serem providos para a correta instalação e prestação dos serviços;
- 14.2.4. A elaboração do Projeto Executivo é de responsabilidade da CONTRATADA e deverá conter as fases do projeto, os cronogramas de execução, e a descrição detalhada dos produtos e subprodutos a serem entregues em cada fase.
 - 14.2.4.1. A conclusão da fase de implantação dos serviços é de até 90 (noventa) dias corridos, contados a partir da data de assinatura do contrato, iniciando-se, a partir de então, a fase de prestação mensal dos serviços, apenas após a emissão do termo de recebimento definitivo.
- 14.2.5. Conter a descrição de topologia lógico e física da rede atual e topologia pretendida em cada etapa;
- 14.2.6. Efetuar o mapeamento de criticidade de todos os ativos envolvidos no projeto, inclusive os de propriedade da CONTRATANTE;
- 14.2.7. Para a implantação dos serviços, indicar de forma detalhada as condições de *Rollback* de cada mudança no ambiente da CONTRATANTE;
- 14.2.8. Estimar o consumo de Unidades de *Rack* (U) e de energia de cada ativo a ser instalado nas dependências da CONTRATANTE, se for o caso;
- 14.3. Os *Softwares* e demais componentes necessários à correta prestação dos serviços deverão:
 - 14.3.1. Conter os recursos necessários e estarem configurados de modo a garantir total operabilidade no ambiente computacional da CONTRATANTE e otimizados para usufruir das melhores condições em termos de desempenho e disponibilidade;
 - 14.3.2. Conter a última versão de *Software* e *Firmware* homologado pelo fabricante;
 - 14.3.3. Ter configuradas senhas de acesso para que a equipe de funcionários designados pelo CONTRATANTE efetue o acesso para a visualização das configurações e *Logs* (acesso seguro e remoto);
 - 14.3.4. Ter configurada senha com direitos totais de administração e configuração a ser utilizada pela CONTRATANTE em caso de emergência;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 14.4. Para aprovação da instalação e configuração de qualquer item que ensejar a emissão de termo de recebimento definitivo, a CONTRATADA deve elaborar relatório técnico com análise dos resultados e impactos decorrentes da atividade executada;
- 14.5. Quando realizadas no ambiente de produção, as atividades poderão ser agendadas para serem executadas após o horário de expediente, a saber, em horários noturnos – após às 20h00 (vinte horas) – além de finais de semana e feriados, conforme disponibilidade da CONTRATANTE;
- 14.6. A operação assistida deverá obedecer aos requisitos a seguir:
- 14.6.1. Iniciará quando forem finalizados o planejamento, a customização de ambiente e a instalação dos ativos de rede, sendo o item de serviço submetido para recebimento definitivo.
- 14.6.2. A mudança para o ambiente de produção será concomitante a este momento, salvo se expressamente solicitado pela CONTRATANTE que seja feita em data diferente. Terá duração de até 30 (trinta) dias corridos, e será executada em Belo Horizonte-MG, nas dependências da CONTRATANTE, em horário comercial (entre 8h30 e 17h30);
- 14.6.3. Caso seja necessária a consecução de atividades pelo técnico responsável pela operação assistida, e que possa afetar a disponibilidade de serviços do ambiente da CONTRATANTE, estas deverão ocorrer após às 20h00 (vinte) horas;
- 14.7. Caso a CONTRATANTE encontre pendências impeditivas à emissão do termo de recebimento definitivo, a operação assistida deverá ser prorrogada até que sejam sanados os motivos geradores das pendências;
- 14.8. Caso a implantação de um serviço cause interferência no funcionamento de qualquer funcionalidade na CONTRATANTE, a CONTRATADA deverá alocar profissionais com qualificação suficiente para corrigir o problema ou retornar o ambiente à condição anterior à implantação, sem quaisquer custos adicionais a CONTRATANTE.
- 14.9. Para todos os componentes da solução, a CONTRATADA deverá implementar e documentar as respectivas configurações de segurança necessárias, que visem à redução do risco de acesso indevido a cada servidor (*Hardening*), como, por exemplo, remoção de serviços desnecessários do sistema operacional, configurações de *Kernel*, configurações dos serviços ativos para suas permissões mínimas de funcionamento, remoção de usuários padrão de sistemas e aplicativos, além de eventuais configurações para resistir a ataques de negação de serviço.
- 14.10. Para o planejamento e o acompanhamento da instalação dos *Softwares* necessários à execução dos serviços, da entrega das etapas para recebimento definitivo, da confecção do Projeto Executivo, da confecção do as-built, e para as demais atividades pertinentes até a emissão do termo de recebimento definitivo de todos os itens, a CONTRATADA deverá alocar GERENTES DE PROJETOS.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

14.11. As qualificações técnicas mínimas exigidas para o perfil de GERENTE DE PROJETO da CONTRATADA são:

Certificações	Descrição
Ao menos uma das certificações de segurança da informação: • Project Management Professional (PMP); • Prince2 Practitioner Certificate in Project Management; • Professional Scrum Master I;	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em gerencia de projetos, com experiência mínima de 12 (doze) meses.

Tabela 11 – Qualificações do Gerente de Projeto

14.11.1. **No momento da assinatura do contrato** será exigido da CONTRATADA a apresentação das documentações do(s) profissional(is) com perfil de GERENTE DE PROJETO, as quais devem comprovar as exigências e obrigações descritas neste Termo de Referência: contrato de prestação de serviços ou carteira de trabalho devidamente assinada pela CONTRATADA, para comprovação de habilidades, e as devidas certificações técnicas para comprovação do conhecimento conforme TABELA de exigências de qualificações.

15. ACORDO DE NÍVEIS DE SERVIÇO

15.1. A prestação dos serviços será baseada no modelo de remuneração em função dos resultados apresentados, em que os pagamentos serão feitos após mensuração e verificação de métricas quantitativas e qualitativas, contendo indicadores de desempenho e metas, com Nível Mínimo de Serviço (NMS) definido em contrato, de modo a resguardar a eficiência e a qualidade da prestação dos serviços.

15.2. Os níveis mínimos de serviço contratados serão registrados, monitorados e comparados às metas de desempenho e qualidade estabelecidas, em termos de prazo e efetividade, condição fundamental para realização dos pagamentos previstos.

15.3. De modo a facilitar a compreensão dos Níveis Mínimos de Serviço (NMS) dos Serviços Gerenciados de Segurança, são apresentadas, a seguir, exigências mínimas em termos de níveis de serviço que devem ser atendidas pela CONTRATADA na execução do contrato, a saber:

15.4. DISPONIBILIDADE MENSAL DOS GRUPOS DE TECNOLOGIAS

15.4.1. Para os itens 1 a 5 dos Serviços Gerenciados de Segurança, a Meta de Disponibilidade Mensal (MDM) por grupo de tecnologia deve ser de, no mínimo:

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

item	Grupo de Tecnologia	MDM (%)	FPI
1	Proteção de Dados e <i>Datacenter</i>	95	1,75
2	Proteção de Dados de <i>Endpoints</i>	95	1,5
4	Visibilidade de Rede e Controle de Incidentes	95	1,5

Tabela 12 – Meta de Disponibilidade Mensal

15.5. O SERVIÇO DE GESTÃO DE DISPONIBILIDADE foi arquitetado para garantir e medir a disponibilidade do parque de segurança da informação descrito neste Termo de Referência. Logo, o mesmo deverá ser utilizado para apurar a meta de disponibilidade mensal (MDM).

15.6. Em cada período avaliado, o cálculo do Percentual de Disponibilidade Mensal (PDM) por item de serviço deve ser calculado com a seguinte fórmula:

$$PDM_k = \frac{[TM - TI_k]}{TM} * 100$$

PDM_k = Percentual de Disponibilidade Mensal do k-ésimo item de serviço;

k = k-ésimo item de serviço;

TM = Tempo total mensal de operação, em minutos, no mês de faturamento;

TI_k = Tempo total mensal de indisponibilidade do k-ésimo item de serviço, em minutos, no mês de faturamento. Devem ser incluídos como Tempo de Indisponibilidade (TI_k):

15.7. Tempo em que o respectivo serviço esteja indisponível ou com desempenho degradado;

15.8. Tempo decorrente entre o início da indisponibilidade do serviço e a sua total recuperação;

15.9. Não devem ser incluídos como Tempo de Indisponibilidade (TI_k):

15.9.1. Falta de energia no local de prestação dos serviços;

15.9.2. Indisponibilidade da rede lógica da CONTRATANTE;

15.9.3. Problemas derivados de ocorrências no ambiente da CONTRATANTE, onde comprovadamente a indisponibilidade não esteja sendo controlada pela CONTRATADA;

15.9.4. Ações necessárias para resolução de problemas que tenham sido autorizadas pelo CONTRATANTE;

15.9.5. Indisponibilidade gerada pela operadora de telecomunicação responsável pelos *Links* e equipamentos do ambiente da CONTRATANTE;

15.9.6. Fatores externos a prestação de serviços, desde que justificado e acordado com o time de segurança da CONTRATANTE;

15.9.7. Indisponibilidade do ambiente virtualizado da CONTRATANTE, infraestrutura computacional em que parte dos *Softwares* que compõem a solução deve ser instalada;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 15.9.8. Manutenções programadas pela CONTRATANTE;
- 15.9.9. Manutenções programadas pela CONTRATADA, desde que previamente autorizadas pela CONTRATANTE.
- 15.9.10. *Tickets* abertos cujo prazo de resolução encerre somente no próximo período de faturamento somente terão calculados os fatores de abatimento a partir do período seguinte;
- 15.10. Os fatores de abatimento por indisponibilidade de serviços (FAIS) relativos ao percentual de disponibilidade mensal deverão, ainda, ser multiplicados por um fator de peso do item (FPI), segundo a **Tabela** - META DE DISPONIBILIDADE MENSAL, por grupo de tecnologia.
- 15.11. O Percentual de Disponibilidade Mensal (PDM) é subsidiário para o cálculo do Fator de Abatimento por Indisponibilidade de Serviço (FAIS), desconto a ser aplicado no valor de prestação mensal de cada conjunto ou item de serviço;
- 15.12. Assim sendo, o Fator de Abatimento por Indisponibilidade de Serviço (FAIS) deve ser calculado de acordo com a seguinte fórmula:

$$FAIS = \sum_{k=1}^{10} VMI_k \times FPI_k \times \left\{ \frac{MDM_k - MIN(MDM_k, PD_k)}{100} \times MTI \right\}$$

Variável	Descrição
k	Número do grupo de tecnologia
FAIS	Fator de abatimento por indisponibilidade de serviço
VMI	Valor mensal do item de serviço de Gestão de Disponibilidade
MDM	Meta de disponibilidade mensal do item
PD	Percentual de disponibilidade mensal, calculada segundo fórmula supracitada.
MTI	Multiplicador por tempo de indisponibilidade, conforme definido a seguir: Valor = 1, se (MDM - PD) menor igual 1; Valor = 1, se (MDM - PD) maior que 1 e menor igual a 5; Valor = 1, se (MDM - PD) for maior que 5;
Min	Função que retorna o valor mínimo.

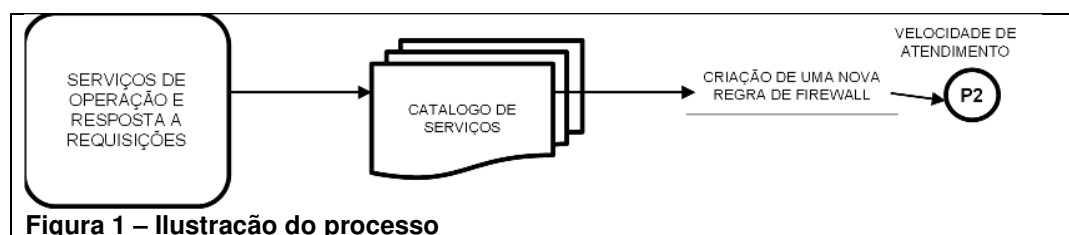
Tabela 13 – Variáveis de Cálculo de Fator de Abatimento por Indisponibilidade de Serviço (FAIS)

15.13. ENTREGA MENSAL DOS SERVIÇOS GERENCIADOS DE SEGURANÇA

- 15.13.1. Além da meta de disponibilidade mensal do parque de segurança da informação do CONTRATANTE, a qual avalia especificamente o **SERVIÇO DE GESTÃO DE DISPONIBILIDADE**, também deverão ser apurados os níveis de serviço para os demais serviços que, somados, compõem o objeto Serviços Gerenciados de Segurança.
- 15.13.2. Todos os serviços que compõem o objeto contratado possuem catálogo de serviço descrito no **ANEXO IV** deste Termo de Referência. Cada item (serviço) que compõe o catálogo de serviço deve estar relacionado com os tipos de velocidade de atendimento descritos na **Tabela**

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

3 deste termo de referência, conforme exemplo ilustrado na figura abaixo:



Tipos	Nível mínimo de serviço (NMS)	IndMeta	Fator de peso da Atividade (FAT)
P1	2 Horas	2 Horas	1
P2	4 Horas	4 Horas	1
P3	8 Horas	8 Horas	0,5
P4	16 Horas	16 Horas	0,5
P5	32 Horas	32 Horas	0,5
P6	64 Horas	64 Horas	0,25
P7	128 Horas	128 Horas	0,25
P8	256 Horas	256 Horas	0,25

Tabela 14 – Níveis de prioridade de Atendimento

- 15.13.3. Em um atendimento onde seja necessária uma janela para execução dos serviços solicitados, o tempo transcorrido entre a necessidade do atendimento e a janela de execução deverão ser excluídos.
- 15.13.4. Os fatores de abatimento por desempenho de serviço (FADS) serão calculados com base na comparação dos resultados alcançados na execução das atividades com os níveis de serviços definidos na TABELA 14 - NIVEIS DE PRIORIDADES DE ATENDIMENTO.
- 15.13.5. O FADS será calculado como somatório das ocorrências realizadas para cada uma das atividades definidas, conforme fórmula a seguir:

$$FADS = \sum_{i=1}^8 \sum_{j=1}^n VMC \times \left[\frac{\text{Max} (INDATINGi.j, INDMETAi) - INDMETAi}{10 \times INDMETAi} \right] \times FPAi$$

Variável	Descrição
I	Tipo de prioridade.
J	Contador de ocorrências do tipo de prioridade que não atenderam o NMS definido.
N	Quantidade de ocorrências do tipo de prioridade que não atenderam o NMS definido.
FADS	Fator de abatimento por desempenho de Serviço
VMC	Valor mensal do contrato.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

INDMETA	Índice de meta (NMS), em minutos/horas/dias, definido para a atividade.
INDATING	Índice atingido, em minutos/horas/dias, pela atividade que ultrapassou o (NMS).
FPA	Fator de peso da atividade.
Max	Função que retorna o valor máximo.

Tabela 15 – Variáveis de Cálculo de Fatores de Abatimento por Desempenho de Serviço (FADS)

16. PAPÉIS E RESPONSABILIDADES

16.1. Durante a vigência contratual, e toda a prestação do serviço objeto desta contratação, deverão ser observados e cumpridos os seguintes papéis e responsabilidades dos profissionais:

16.1.1. **Fiscal técnico do contrato (CONTRATANTE):** responsável pelo acompanhamento, fiscalização e avaliação da execução do objeto nos moldes contratados, observando o fiel cumprimento de todas as cláusulas contratuais.

16.1.2. **Gestor do contrato (CONTRATANTE):** responsável pela coordenação das atividades relacionadas à fiscalização, bem como dos atos preparatórios à instrução processual e da formalização dos procedimentos referentes aos aspectos que envolvam a prorrogação, a alteração, o reequilíbrio, o pagamento, eventuais aplicações de sanções e extinção dos contratos, dentre outras ações.

16.1.3. **Preposto (CONTRATADA):** é o profissional indicado pelo Fornecedor de Serviço para representá-la administrativa e tecnicamente. É o responsável pela coordenação operacional das atividades previstas nos projetos, de forma a solucionar qualquer dúvida, conflito ou desvio técnico que possa comprometer a execução das OS. Deverá ter bons conhecimentos em gestão de projetos para garantir o controle sobre os sinais vitais de cada projeto. Também é responsável pela interlocução com o Gestor do Contrato do CONTRATANTE.

16.2. As qualificações técnicas exigidas para o perfil de PREPOSTO da CONTRATADA:

Certificações	Descrição
Ao menos uma das certificações de segurança da informação: • CISSP (Certified Information Systems Security Professional); • CISM (Certified Information Security Manager); • CIA (Certified Intrusion Analyst), • GSEC (GIAC Security Essentials); • GCIH (GIAC Incident Handler) • GMON (GIAC Continuous Monitoring);	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência mínima de 12 (doze) meses em coordenação e gestão de contratos de serviços continuados.

Tabela 16 – Certificações e Qualificações do Preposto

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 16.3. **No momento da assinatura do contrato** será exigido da CONTRATADA a apresentação das documentações do(s) profissionais com perfil de PREPOSTO as quais devem comprovar as exigências e obrigações descritas neste termo de referência: contrato de prestação de serviços ou carteira de trabalho devidamente assinada pela CONTRATADA para comprovação de habilidades e as devidas certificações técnicas para comprovação do conhecimento conforme TABELA 16.

17. ESCOPO E PRAZOS DE EXECUÇÃO E DE ACEITE E NATUREZA DOS SERVIÇOS

- 17.1. O período de prestação dos serviços, a partir da emissão do termo de recebimento definitivo será o estabelecido na tabela abaixo:

LOTE	ITEM	DESCRIÇÃO	QTD	MÉTRICA	PERÍODO
1	1	Serviço de Monitoramento de Ataques Cibernéticos e Resposta A Incidentes	1	500 EPS*	60
	2	Serviço de Gestão de Vulnerabilidades	300	Ativos	60
	3	Serviço de Monitoramento, Detecção e Resposta a Incidentes para Endpoint	130	Ativos	60

*EPS - Eventos por Segundo - é uma métrica utilizada pelo mercado para dimensionar o SIEM (equipamento responsável pela coleta, análise e correlacionamento dos Logs).

- 17.2. SERVIÇOS GERENCIADOS DE SEGURANÇA – DEMANDA FUTURA serão demandados de acordo com as necessidades da CONTRATANTE, solicitados por meio de Ordem de Serviço cuja execução deve ser recebida por meio do Termo de Recebimento de Serviços.
- 17.3. A partir da assinatura do contrato, correrão os seguintes prazos:
- 17.4. Reunião de início do projeto (*Kick-Off*): a ser realizada em até 10 (dez) dias corridos após a assinatura do contrato. Deverá ser previamente agendada pela **CONTRATADA** com 02 (dois) dias úteis de antecedência.
- 17.5. Entrega do Projeto Executivo: até 30 (trinta) dias corridos, contados a partir da reunião de início do projeto (*Kick-Off*);
- 17.6. A CONTRATANTE se manifestará no prazo de até 10 (dez) dias corridos, contados da data de entrega do Projeto Executivo;
- 17.7. Havendo necessidade de ajustes, a CONTRATADA terá até 10 (dez) dias corridos para realizá-los, contados da notificação a ser efetuada pela CONTRATANTE, a respeito da manifestação sobre o Projeto Executivo;
- 17.8. A conclusão da fase de implantação dos serviços é de até 90 (noventa) dias corridos, contados a partir da data de início da vigência do contrato, mediante a emissão do termo de recebimento definitivo pela CONTRATANTE.
- 17.9. O termo de recebimento definitivo obedecerá os seguintes critérios:

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 17.10. A CONTRATANTE terá 15 (quinze) dias corridos para emitir o termo de recebimento definitivo depois de finalizado o planejamento, customização e a instalação do ambiente;
- 17.11. A prestação dos serviços mensais iniciará somente a partir da emissão do termo de recebimento definitivo pela CONTRATANTE;
- 17.12. Para todos os bens importados, caso necessário, por parte da CONTRATADA, que sejam instalados nas dependências da CONTRATANTE, será necessária a apresentação dos respectivos comprovantes de origem.
- 17.13. O Centro de Operações de Segurança da CONTRATADA deverão estar em pleno funcionamento, operando em regime 24x7x365, em até 75 (setenta e cinco) dias corridos, contados da data de início da vigência contratual.

18. INSPEÇÕES E DILIGÊNCIAS

- 18.1. A CONTRATANTE reserva-se o direito de efetuar inspeções e diligências para sanar quaisquer dúvidas existentes, podendo efetuá-las previamente à contratação;
- 18.2. A CONTRATANTE poderá realizar diligência no Centro de Operações de Segurança da CONTRATADA antes do início da prestação do serviço, *in loco*, a fim de validar e aferir se TODOS os itens solicitados neste Termo de Referência serão atendidos;
- 18.3. A contratação não será formalizada, caso **não** haja o atendimento de quaisquer itens previstos neste Termo de Referência.
- 18.4. As Diligências não poderão ser restritas a dias e horários específicos, sendo possível que a mesma seja executada em horários fora do chamado “horário comercial”, sendo possível a visitação em finais de semana, períodos noturnos e afins;
- 18.5. A CONTRATADA poderá restringir a quantidade de pessoas presentes na diligência, porém ela deverá apresentar durante a visita todas as comprovações necessárias, todos os processos solicitados e responder a todos os questionamentos.
- 18.6. Em caso de eventos adversos que impossibilitem a diligência a contratada deverá prover acesso de maneira remota e virtual para a verificação dos itens a serem inspecionados.

19. TRATAMENTO DE INCIDENTES CIBERNÉTICOS

- 19.1. É de responsabilidade da CONTRATADA a restauração dos serviços comprometidos através da definição de estratégias e de ações para conter o incidente; a erradicação dos artefatos maliciosos do ambiente do CRCMG; a recuperação dos serviços dependentes de tecnologia; bem como ações que terão como objetivo mitigar riscos existentes para evitar com que incidentes semelhantes ocorram no futuro.
- 19.1.1. É de responsabilidade da CONTRATANTE contactar as suas terceirizadas para atendimento

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

das estratégias e ações repassadas pela CONTRATADA para completo restabelecimento do ambiente o mais rápido e seguro.

19.1.1.1. Serviços de responsabilidade da CONTRATANTE:

- a) Restauração de Backups de servidores, serviços, dados, banco de dados, configurações do AD, senhas, GPOs, grupos;
- b) Configuração do Firewall;

19.2. Os serviços a serem executados, culminarão na entrega pela contratada dos seguintes documentos:

19.2.1. **Relatório executivo** – Demonstrará a conformidade e riscos antes da aplicação dos controles de segurança e após a aplicação dos controles de segurança;

19.2.2. **Relatório técnico** – Demonstrará tecnicamente os controles aplicados e o nível de conformidade individual de cada estação de trabalho e servidor, abrangendo:

19.2.2.1. Tratamento de incidentes: ações realizadas para mitigação dos riscos;

19.2.2.2. Relatório forense: Relatório demonstrando as ações do ator de ameaça;

19.2.2.3. Principais riscos: Principais riscos identificados;

19.2.2.4. Plano Diretor: Plano de ação e recomendações para lidar com os riscos residuais;

19.3. A CONTRATADA deverá emitir relatórios técnicos e auxiliar o CRCMG na elaboração de respostas às autoridades competentes, quando necessário e a critério do CRCMG, no caso de eventual incidente de segurança da informação.

20. MODALIDADE DA LICITAÇÃO

Pregão Eletrônico.

21. VALOR DE REFERÊNCIA

21.1. O valor de referência, que corresponde ao **VALOR GLOBAL MÁXIMO** que o CRCMG se propõe a pagar pela prestação dos serviços, objeto deste Termo de Referência, pelo período de 60 (sessenta) meses é de R\$ 872.250,00 (oitocentos e setenta e dois mil duzentos e cinquenta reais).

VALOR DE REFERÊNCIA	
Estimativa Mensal	Estimativa Global 60 meses
R\$ 14.537,50	R\$ 872.250,00

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- 21.2. No valor que vir a oferecer deverão ser incluídas todas as despesas com os profissionais e equipamentos, bem como, taxas, alimentação, transporte, hospedagem, enfim, todos os encargos fiscais, comerciais, trabalhistas e previdenciários, resultantes da prestação dos serviços objeto deste Procedimento.

22. CRITÉRIO DE JULGAMENTO DAS PROPOSTAS

- 22.1. No julgamento das propostas, será considerada vencedora a que apresentar **MENOR PREÇO GLOBAL**, desde que atendidas às especificações constantes deste Edital e de seus Anexos.
- 22.2. Será desclassificada a proposta que, para sua viabilização, apresente vantagens ou subsídios que não estejam previamente autorizados em lei, assim como as que não se encontrem em conformidade com os requisitos estabelecidos no presente Edital.
- 22.3. O julgamento das propostas será de acordo com a sistemática do site de compras denominado www.comprasnet.gov.br, em consonância com a legislação vigente.

23. DO PRAZO DE VIGÊNCIA DO CONTRATO

O contrato vigorará pelo prazo de 60 (sesenta) meses, a contar da data de sua assinatura e será regido pelas Leis nº 10.520/02, nº 8.666/93 e pelo Código Civil Brasileiro.

24. DA GARANTIA CONTRATUAL

- 24.1. A CONTRATADA, no prazo de até 20 (vinte) dias, contado a partir da data de assinatura deste contrato, prestará garantia de cumprimento das obrigações contratuais, correspondente a 5 % (cinco por cento) do valor estimado para a execução dos serviços, objeto deste contrato.
- 24.1.1. O prazo estipulado no subitem anterior poderá ser prorrogado por igual período, a juízo do CRCMG, à vista das justificativas que lhe forem apresentadas pela CONTRATADA.
- 24.1.2. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa, nos termos do item 25.2.4.5.
- 24.1.3. O atraso superior a 30 (trinta) dias corridos, após os prazos previstos nos subitens 24.1 e 24.1.1, autoriza a CONTRATANTE a promover a rescisão deste contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os incisos I e II do art. 78 da Lei nº 8.666/1993, sem prejuízo de outras sanções previstas na Lei e neste contrato.
- 24.2. Caberá à CONTRATADA escolher uma das modalidades previstas no art. 56 da Lei nº 8.666/1993:
- a) caução em dinheiro ou títulos da dívida pública;
 - b) seguro-garantia;
 - c) fiança bancária.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

24.3. Em se tratando de garantia prestada por meio de caução em dinheiro, o depósito deverá ser feito obrigatoriamente na Caixa Econômica Federal, conforme determina o art. 82 do Decreto n.º 93.872/1986, em caderneta de poupança, em favor do CRCMG, e será corrigida pelos índices oficiais aplicados à essa modalidade de depósito bancário.

24.4. Se a opção for pelo seguro-garantia:

a) a apólice indicará o CRCMG como beneficiário, devendo ser emitida por instituição autorizada pela Superintendência de Seguros Privados (SUSEP) a operar no mercado securitário, que não se encontre sob regime de direção fiscal, intervenção, liquidação extrajudicial ou fiscalização especial e que não esteja cumprindo penalidade de suspensão imposta pela autarquia;

b) seu prazo de validade deverá corresponder ao período de vigência deste contrato, acrescido de 90 (noventa) dias para apuração de eventual inadimplemento da CONTRATADA, ocorrido durante a vigência contratual, e para a comunicação da expectativa de sinistro ou do efetivo aviso de sinistro à instituição emitente, observados os prazos prescricionais pertinentes;

c) a apólice deve prever expressamente responsabilidade da seguradora por todas e quaisquer multas de caráter sancionatório aplicadas à CONTRATADA.

24.5. Se a opção for pela fiança bancária, o instrumento de fiança deve:

a) ser emitido por instituição financeira que esteja autorizada pelo Banco Central do Brasil a funcionar no Brasil e que não se encontre em processo de liquidação extrajudicial ou de intervenção da autarquia;

b) ter prazo de validade correspondente ao período de vigência deste contrato, acrescido de 90 (noventa) dias para apuração de eventual inadimplemento da CONTRATADA, ocorrido durante a vigência contratual, e para a comunicação do inadimplemento à instituição financeira, observados os prazos prescricionais pertinentes;

c) ter afirmação expressa do fiador de que, como devedor solidário, fará o pagamento ao CRCMG, independentemente de interpelação judicial, caso o afiançado não cumpra suas obrigações;

d) ter renúncia expressa do fiador ao benefício de ordem e aos direitos previstos nos arts. 827 e 838 do Código Civil Brasileiro.

24.6. Se a opção for pelo título da dívida pública, este deverá:

a) ter sido emitido sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil;

b) ser avaliado por seu valor econômico, conforme definido pelo Ministério da Economia.

24.7. A garantia, qualquer que seja a modalidade escolhida, assegurará o pagamento de:

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- a) prejuízos advindos do não cumprimento do objeto deste contrato e do não adimplemento das demais obrigações nele previstas;
- b) prejuízos causados ao CRCMG ou a terceiro, decorrentes de culpa ou dolo durante a execução deste contrato;
- c) multas moratórias e punitivas aplicadas pelo CRCMG à CONTRATADA; e
- d) obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza, não adimplidas pela CONTRATADA.
- 24.7.1. A modalidade seguro garantia somente será aceita se contemplar todos os eventos indicados no subitem 24.7.
- 24.8. Não serão aceitos seguro-garantia ou fiança bancária que contenham cláusulas contrárias aos interesses do CRCMG.
- 24.9. Sem prejuízo das sanções previstas em lei e neste contrato, a não prestação da garantia exigida implicará sua imediata rescisão.
- 24.10. Se o valor da garantia vier a ser utilizado, total ou parcialmente, no pagamento de qualquer obrigação vinculada a este ajuste, incluída a indenização a terceiros, a CONTRATADA deverá proceder à respectiva reposição, no prazo máximo de 20 (vinte) dias, contados da data do recebimento da notificação do CRCMG.
- 24.11. Se houver acréscimo ao valor deste contrato, a CONTRATADA se obriga a fazer a complementação da garantia no prazo máximo 20 (vinte) dias, contados da data do recebimento da notificação do CRCMG.
- 24.12. Na hipótese de prorrogação deste contrato, o CRCMG exigirá nova garantia, escolhida pela CONTRATADA entre as modalidades previstas na Lei n.º 8.666/1993.
- 24.13. O documento de constituição da nova garantia deverá ser entregue ao CRCMG no prazo máximo de 20 (vinte) dias, contados da data de assinatura do respectivo termo aditivo.
- 24.14. A garantia, ou seu saldo, será liberada ou restituída, a pedido da CONTRATADA, no prazo de 90 (noventa) dias após o término do prazo de vigência deste contrato, mediante certificação, por seu gestor ou fiscal, de que os serviços foram realizados a contento e desde tenham sido cumpridas todas as obrigações aqui assumidas.
- 24.15. A qualquer tempo, mediante entendimento prévio com o CRCMG, poderá ser admitida a substituição da garantia, observadas as modalidades previstas no subitem 24.2 deste contrato.
- 24.15.1. Aceita pelo CRCMG, a substituição da garantia será registrada no processo administrativo por meio de apostilamento.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

25. DAS SANÇÕES ADMINISTRATIVAS

25.1. Comete infração administrativa nos termos da Lei nº 10.520 de 2002 e da Lei nº 8.666/1993, a CONTRATADA que:

- 25.1.1. inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;
- 25.1.2. ensejar o retardamento da execução do objeto;
- 25.1.3. falhar ou fraudar na execução do contrato;
- 25.1.4. comportar-se de modo inidôneo; ou
- 25.1.5. cometer fraude fiscal.

25.2. Pela inexecução total ou parcial do objeto deste contrato ou descumprimento de obrigações, a Administração poderá aplicar à CONTRATADA as seguintes sanções:

- 25.2.1. **Advertência por escrito**, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado;
- 25.2.2. **Suspensão temporária do direito de participar de licitação e impedimento de contratar** com a Administração, pelo prazo de até 2 (dois) anos;
- 25.2.3. **Impedimento de licitar e contratar** com órgãos e entidades da União, com o consequente descredenciamento no SICAF pelo prazo de até 5 (cinco) anos.
- 25.2.4. **Multa de:**
 - 25.2.4.1. 0,5% (cinco décimos por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, limitada a incidência a 15 (quinze) dias. Após o décimo quinto dia e a critério da Administração, no caso de entrega com atraso, poderá ocorrer a não aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença;
 - 25.2.4.2. 10% (dez por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;
 - 25.2.4.3. em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida;
 - 25.2.4.4. 3% (três por cento), 5% (cinco por cento) ou 10% (dez por cento), sobre o valor total da contratação, em caso de descumprimento de obrigações assumidas, por ocorrência, conforme a gradação estabelecida nos subitens e tabela abaixo.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

25.2.4.5. 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso na apresentação da garantia (seja para reforço ou por ocasião de prorrogação), observado o máximo de 2% (dois por cento). O atraso superior a 25 (vinte e cinco) dias autorizará a Administração CONTRATANTE a promover a rescisão do contrato;

25.3. Na aplicação das sanções, o CRCMG levará em consideração a efetiva gravidade da conduta do infrator, o caráter educativo da pena, bem como, o real dano causado ao Conselho. Sendo assim, as multas e outras sanções aplicadas só poderão ser relevadas, motivadamente, por conveniência administrativa.

25.4. As FALTAS LEVES serão puníveis com a aplicação da penalidade de advertência e/ou multa, no percentual de 3% (três por cento), caracterizando-se pelo descumprimento parcial de deveres de pequena monta, assim entendidas como aquelas que não acarretam prejuízos relevantes aos serviços da Administração e a despeito delas, a regular prestação dos serviços não fica inviabilizada.

25.5. As FALTAS MÉDIAS serão puníveis com a aplicação da penalidade de multa no percentual de 5% (cinco por cento), caracterizando-se pela recorrência de quaisquer FALTAS LEVES ou pelo descumprimento parcial ou total de obrigação que acarrete prejuízos aos objetivos da Administração, mas sem inviabilizar total ou parcialmente a execução dos serviços.

25.6. As FALTAS GRAVES serão puníveis com a aplicação das penalidades de multa no percentual de 10% (dez por cento), podendo ser aplicada cumulativamente as sanções de suspensão temporária do direito de participar em licitação e impedimento de contratar com a Administração ou impedimento de licitar e contratar com órgãos e entidades da União, caracterizando-se pela recorrência de quaisquer FALTAS MÉDIAS ou pelo descumprimento parcial ou total de obrigação que acarrete prejuízos relevantes aos objetivos da Administração, inviabilizando a execução da contratação em decorrência de conduta culposa ou dolosa da contratada.

25.7. Afim de nortear na efetiva aplicabilidade das gradações que tratam nos subitens acima, será utilizada a seguinte classificação:

TIPO DE FALTA	GRAVIDADE
Veicular qualquer tipo de publicidade acerca do Contrato, salvo se houver prévia autorização da Administração do Conselho.	LEVE
Abster-se de prestar as informações e esclarecimentos que venham a ser solicitados pelo CRCMG, atendendo às solicitações nos prazos especificados.	LEVE
Não disponibilizar uma conta de e-mail para fins de comunicação entre as partes, bem como, endereço comercial e telefone de contato ou, em caso de alteração, não comunicar prontamente ao CRCMG.	MÉDIA
Alocar, na prestação dos serviços, profissionais com formação e qualificações não adequadas ou incompatíveis com a prestação dos serviços, conforme estabelecido no Termo de Referência.	MÉDIA

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

Utilizar empregado sem qualificação para a execução dos serviços ou, em caso de desligamento, não proceder à pronta substituição por outro profissional com a formação e qualificações estabelecidas no Termo de Referência.	MÉDIA
Provocar, por meio de seus empregados e representantes, qualquer dano patrimonial ou à imagem e reputação do CRCMG.	MÉDIA
Não substituir, após solicitação do CRCMG, empregado que tenha conduta inconveniente ou incompatível com suas atribuições.	MÉDIA
Prestar os serviços sem obedecer estritamente às condições estabelecidas neste Termo de Referência e no Contrato pactuado.	GRAVE
Não cumprir os prazos de entrega e execução dos serviços estipulados neste Termo de Referência.	GRAVE
Não providenciar a imediata correção das deficiências apontadas pelo fiscal do Contrato, quanto à execução contratual.	GRAVE
Deixar de manter todas as condições de habilitação e qualificação que ensejaram sua contratação, durante todo o período de vigência do Contrato.	GRAVE
Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços contratados.	GRAVE

25.7.1. As faltas cometidas pela Contratada que não se enquadrarem em nenhuma das ocorrências previstas na tabela acima, serão avaliadas caso a caso, no âmbito do Processo Administrativo.

25.7.2. Ao longo do período de validade da Ata, de 12 meses, o acúmulo de condutas faltosas cometidas de forma reiterada, de mesma classificação ou não, bem como as reincidências, ensejará a aplicação, pela administração de penalidades relacionadas às faltas de maior gravidade, considerando que, o fato de a Administração relevar qualquer falta, não implicará em novação.

25.8. Reserva-se ao CRCMG o direito de reter e compensar, dos pagamentos da contratada, as multas referidas nos subitens anteriores, assegurado o contraditório e a apresentação de defesa prévia, nos termos da legislação vigente.

25.9. As sanções previstas nos subitens 25.2.1, 25.2.2 e 25.2.3 poderão ser aplicadas à CONTRATADA cumulativamente com as multas previstas no subitem 25.2.4.

25.10. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

25.10.1. tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

25.10.2. tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

25.10.3. demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

25.11. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

25.11.1. As partes concordam que o envio e o recebimento das notificações e comunicações em geral, inclusive no âmbito de processo administrativo que venha a ser instaurado, serão realizados por meio de e-mail.

25.12. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

25.13. As penalidades serão obrigatoriamente registradas no SICAF.

25.14. Além das sanções acima previstas, o contrato poderá ser rescindido pelos motivos previstos nos artigos 77 a 80 da Lei nº 8.666/93.

26. OBRIGAÇÕES DA CONTRATADA

26.1. Prestar os serviços, objeto deste Edital, cumprindo os prazos e atendendo integralmente a todas condições e especificações estabelecidas neste Termo de Referência.

26.2. Entregar os serviços objeto desse Edital, obedecendo aos prazos estipulados neste Termo de Referência.

26.3. Arcar com todos os custos necessários à execução dos serviços, objeto deste procedimento, tais como materiais, softwares e equipamentos, alimentação, transporte, hospedagem, instalações, mão de obra e quaisquer outros que forem pertinentes ao cumprimento do objeto, em conformidade com este Termo de Referência.

26.4. Assumir e cumprir todas as obrigações trabalhistas previstas em legislação e normas específicas, responsabilizando-se, exclusivamente, pela remuneração, encargos sociais e previdenciários, benefícios e demais despesas referentes a seus profissionais, tendo em vista que não será estabelecido nenhum vínculo empregatício ou de responsabilidade entre os profissionais disponibilizados para a execução dos serviços contratados e o CRCMG.

26.5. Responsabilizar-se pela idoneidade e pelo comportamento de seus empregados, prepostos ou subordinados.

26.6. Utilizar, na execução dos serviços, somente profissionais especializados e, em caso de desligamento, promover a reposição do profissional por outro com a mesma formação e qualificações estabelecidas neste Termo de Referência.

26.7. Reparar, corrigir, remover ou substituir às suas expensas, no total ou em parte, o objeto deste procedimento em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

materiais empregados, no prazo de 48 (quarenta e oito) horas da notificação, sem ônus par ao CRCMG.

- 26.8. Prestar todos os esclarecimentos que forem solicitados pelo CRCMG, atendendo de imediato às solicitações de seus representantes.
- 26.9. Informar, de imediato, as alterações de endereço, de número de telefones e de e-mails.
- 26.10. Assumir inteira responsabilidade, civil, administrativa e penal por danos materiais ou pessoais causados ao CRCMG e/ou a terceiros provocados por ineficiência ou irregularidades cometidas por seus empregados, contratados ou prepostos envolvidos na execução do contrato, decorrentes de dolo ou culpa.
- 26.11. Guardar o mais absoluto sigilo em relação às informações ou documentos de qualquer natureza a que venham tomar conhecimento, respondendo, administrativa, civil e criminalmente por sua indevida divulgação e/ou incorreta ou descuidada utilização.
- 26.11.1. A CONTRATA deverá apresentar, o momento de assinatura do contrato, Termo de Confidencialidade e Sigilo do Prestador, constante do Anexo VIII do Edital.
- 26.12. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, observando a prática da boa técnica e a legislação vigente.
- 26.13. Emitir as notas fiscais com as devidas deduções legais, devendo ser apresentada, juntamente, com as certidões de regularidade junto ao FGTS, ao INSS e à Justiça do Trabalho, além da Declaração de Optante pelo Simples Nacional, se for o caso.
- 26.14. Manter, durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas neste Edital.
- 26.15. Aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até 25% (vinte e cinco por cento) do valor inicial do contrato, na forma da legislação vigente.
- 26.16. Submeter-se à fiscalização do CRCMG, na execução dos serviços, seguindo todas as orientações repassadas.

27. OBRIGAÇÕES DO CRCMG

- 27.1. Proporcionar as condições necessárias à execução dos serviços ora contratados, assim como prestar, prontamente, as informações e os esclarecimentos que venham a ser solicitados pela contratada;
- 27.2. Efetuar o pagamento à contratada, de acordo com as condições de preço e prazo estabelecidas no contrato.



Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

27.3. Acompanhar e fiscalizar o andamento dos serviços, por intermédio do funcionário do CRCMG designado como Fiscal do Contrato.

27.4. Rejeitar, no todo ou em parte, os serviços entregues em desacordo com as obrigações assumidas pela empresa contratada.

27.5. Comunicar a contratada toda e qualquer ocorrência relacionada com a execução do serviço.

27.6. Notificar a contratada, por escrito e com antecedência, sobre multas, penalidades e quaisquer débitos de sua responsabilidade.

28. SUBCONTRATAÇÃO

Não será admitida a subcontratação do objeto licitatório.

29. ALTERAÇÃO SUBJETIVA

28.1. É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa do Contratante à continuidade do contrato.

30. RESPONSÁVEIS PELO TERMO DE REFERÊNCIA

O presente Termo de Referência foi elaborado pela Gerência de Tecnologia da Informação e pela Gerência Administrativa e Financeira (GEADF) em consonância com as disposições legais e normativas aplicáveis e com o interesse e a conveniência da Administração, sendo objeto de exame e aprovação do Ordenador de Despesa do Conselho, e passará a integrar o processo administrativo formalizado visando à instauração do certame licitatório e a efetividade da contratação.

DATA

ASSINATURA DO GERENTE DE TECNOLOGIA DA INFORMAÇÃO

xxxxxxxxxxxxx/2023

DATA

ASSINATURA DO GERENTE ADMINISTRATIVO E FINANCEIRO

xxxxxxxxxxxxx/2023

DATA

ASSINATURA DO PRESIDENTE DO CRCMG

xxxxxxxxxx/2023



Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

ANEXO II – MODELO DE PROPOSTA

Ao
CONSELHO REGIONAL DE CONTABILIDADE DE MINAS GERAIS

PREGÃO ELETRÔNICO Nº 0XX/2023

EMPRESA: _____

CNPJ: _____

ENDEREÇO: _____

TELEFONE: _____

(E-MAIL): _____

Em atendimento ao Edital do Pregão em epígrafe, apresentamos a(s) seguinte(s) proposta(s) de preços.

ITEM I	
OBJETO: CONTRATAÇÃO DE EMPRESA ESPECIALIZADA EM SERVIÇOS GERENCIADOS DE SEGURANÇA, INCLUINDO:	
1. Serviços de monitoramento de ataques cibernéticos e resposta a incidentes:	
1.1. Visa o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados à CONTRATANTE, através de fornecimento de solução de correlacionamento de logs de aplicações, serviços e infraestrutura do CONTRATANTE, que possam gerar eventos de segurança da informação, aos quais devem ser analisados, remediados, contidos e documentados, podendo estes serem transformados em um incidente de segurança da informação, obedecendo um processo cíclico e rigoroso de gestão de eventos.	
2. Serviços de Gestão de Vulnerabilidades:	
2.1. Visando, de forma proativa e recorrente, identificar possíveis vulnerabilidades de segurança da informação na infraestrutura, nas aplicações e nas contas de usuários do CONTRATANTE, a fim de evitar que ataques cibernéticos direcionados à CONTRATANTE obtenha sucesso, explorando tais vulnerabilidades já conhecidas.	
3. Serviço de monitoramento, detecção e resposta a incidentes para Endpoints.	
3.1. Visando à proteção, monitoramento contínuo e operação de solução dedicada a proteção de estações e servidores do CONTRATANTE, realizando de forma proativa o bloqueio de códigos maliciosos tipo vírus, Malware - blindando os ativos protegidos também contra Ransomware, oferecendo possibilidade de realização de "Rollback" de arquivos alvos de códigos maliciosos, oferecendo ainda suporte à investigação de ataques através da trilha de registros de eventos forense.	
Os serviços serão prestados em total conformidade com as condições, detalhamento e especificações constantes do Termo de Referência Anexo I do Edital nº 0xx/2023.	
VALOR MENSAL	R\$ (.....)
VALOR GLOBAL PERÍODO DE 60 (SESSENTA MESES)	R\$ (.....)



Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

Validade da Proposta: 60 (sessenta) dias.

Condições de pagamento: O CRCMG efetuará o pagamento em até 10 (dez) dias úteis, após a prestação dos serviços, mediante apresentação da nota fiscal, com as devidas deduções legais, bem como das certidões de regularidade junto ao FGTS, ao INSS e à Justiça do Trabalho, além da Declaração de Optante pelo Simples Nacional, se for o caso.

Serão descontados sobre os pagamentos a serem realizados, as devidas retenções de tributos e contribuições, conforme determina a Instrução Normativa nº. 1.234, de 11/01/2012, da Secretaria da Receita Federal.

Submetemo-nos a todas as condições do Edital nº 0XX/2023, inclusive quanto ao cumprimento na íntegra do respectivo Termo de Referência - Anexo I.

Dados do representante legal da empresa, responsável pela assinatura do Contrato:

Nome:

Função:

CPF:

Telefone/Fax:

Endereço Eletrônico (e-mail):

_____ de _____ de 2023.

Assinatura do representante legal da empresa

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

ANEXO III - MINUTA DE CONTRATO

Contrato de prestação de serviços que entre si fazem, de um lado, o **CONSELHO REGIONAL DE CONTABILIDADE DE MINAS GERAIS**, com sede em Belo Horizonte, Minas Gerais, na Rua Cláudio Manoel, 639, Bairro Savassi, inscrito no CNPJ/MF sob o número 17.188.574/0001-38, representado por seu presidente, Contador XXXXXXXXXXXX, de ora em diante denominado CRCMG, e, de outro, XXXXXXXXXXXX, com sede em XXXXXXXXXXXX, XXXXXXXXXXXX, na Rua/AVXXXXXXXX, nº XXXX, Bairro XXXX, inscrita no CNPJ sob o nº XXXXXX, neste ato representado por seu representante legal, XXXXXXXX, de ora em diante denominada CONTRATADA, sujeitando as partes contratantes às normas constantes na Lei nº 10.520, de 17/7/2002, Lei nº 13.709, de 14/8/2018, Lei Complementar nº 123, de 13/12/2006 e Decreto nº 8.538, de 06/10/2015, com aplicação subsidiária das normas da Lei nº 8.666, de 21/06/93, mediante as cláusulas e condições que se seguem:

CLÁUSULA PRIMEIRA - DO OBJETO

1. Contratação de empresa especializada na prestação de SERVIÇOS GERENCIADOS DE SEGURANÇA, conforme condições e especificações estabelecidas no Anexo I – Termo de Referência deste Edital, conforme condições e especificações estabelecidas no Edital nº 0XX/2023 e seu Anexo I – Termo de Referência.

CLÁUSULA SEGUNDA - OBRIGAÇÕES DA CONTRATADA E DO CRCMG

2.1. As obrigações da CONTRATADA e do CRCMG são aquelas previstas no Termo de Referência, Anexo I do Edital Pregão Eletrônico nº 0XX/2023.

CLÁUSULA TERCEIRA - DOS PREÇOS

3.1. Pela execução dos serviços objeto deste contrato o CRCMG pagará a CONTRATADA o valor mensal de R\$ (.....), cujo desembolso dar-se-á com recursos previstos em dotação orçamentária própria, sob a rubrica 6.3.1.3.02.01.005, observado o item 4.1 deste contrato.

3.2. O valor global pela prestação dos serviços no período de 60 (sessenta) meses é de R\$ (.....), observado o item 4.1 deste contrato.

3.3. Serão descontados sobre os pagamentos a serem realizados, as devidas retenções de tributos e contribuições, conforme determina a Instrução Normativa nº. 1.234, de 11/01/2012, da Secretaria da Receita Federal.

3.4. Os preços são fixos e irredutíveis no prazo de um ano contado da data limite para a apresentação das propostas.

3.4.1. Dentro do prazo de vigência do contrato e mediante solicitação da contratada, os preços contratados poderão sofrer reajuste após o interregno de um ano, aplicando-se o índice IPCA, acumulado nos 12 (doze) meses anteriores a data base ou outro índice que venha a substituí-lo, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

3.4.2. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

CLÁUSULA QUARTA - DAS CONDIÇÕES DE PAGAMENTO

4.1. Os pagamentos terão início somente após a instalação da solução e a completa disponibilização dos serviços, mediante o aceite definitivo da CONTRATANTE.

4.1.1. O CRCMG efetuará o pagamento em até 10 (dez) dias úteis, contados a partir do recebimento da Nota Fiscal com as devidas deduções legais.

4.1.2. Considera-se ocorrido o recebimento da nota fiscal ou fatura no momento em que o órgão contratante atestar a execução do objeto do contrato.

4.1.3. A Nota Fiscal deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da Lei nº 8.666, de 1993.

4.2. Serão descontados sobre o pagamento a ser realizado, as devidas retenções de tributos e contribuições, conforme determina a Instrução Normativa nº. 1.234, de 11/01/2012, da Secretaria da Receita Federal.

4.3. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante;

4.4. Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

4.5. Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante.

4.6. Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018.

4.7. Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

4.8. Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

4.9. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.

4.10. Será rescindido o contrato em execução com a contratada inadimplente no SICAF, salvo por motivo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante.

4.11. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

$EM = I \times N \times VP$, sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

$$I = (TX) \quad I = \frac{(6 / 100)}{365}$$

$$TX = \text{Percentual da taxa anual} = 6\% \\ I = 0,00016438$$

CLÁUSULA QUINTA - DA VIGÊNCIA

5.1. O presente contrato vigorará pelo prazo de 60 (sessenta) meses, a contar da data de sua assinatura e será regido pelas Leis nº 10.520/2002, nº 8.666/93 e pelo Código Civil Brasileiro.

CLÁUSULA SEXTA - DO ACOMPANHAMENTO E FISCALIZAÇÃO

6.1. O contrato será acompanhado e fiscalizado conforme critérios e condições estabelecidos no Termo de Referência – Anexo I do Edital Pregão Eletrônico nº 0XX/2023, observadas as designações específicas.

CLÁUSULA SÉTIMA - DAS SANÇÕES

7.1. As sanções relacionadas à execução do contrato são aquelas previstas no Termo de Referência, Anexo I do Edital Pregão Eletrônico nº 0XX/2023.

CLÁUSULA OITAVA - DA RESCISÃO

8.1. O contrato poderá ser rescindido pelos motivos previstos nos artigos 77 a 80 da Lei nº 8.666/93.

CLÁUSULA NONA - DA CONFORMIDADE COM A LEI GERAL DE PROTEÇÃO DE DADOS

9.1. A Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, (LGPD), é a legislação brasileira que regula as atividades de tratamento de dados pessoais. O CRCMG seguindo as boas práticas de governança e *compliance* está comprometido com seus deveres de garantia da privacidade e de proteção de dados pessoais, e preza em todas as relações contratuais que os envolvidos adotem boas práticas de governança, visando sempre o interesse do respeito a legislação vigente.

9.2. Neste sentido, a CONTRATADA declara estar ciente que a CONTRATANTE é uma entidade de fiscalização tendo como uma de suas atividades precípuas, o registro de categoria profissional, regida pelo princípio do acesso à informação normatizado pela Lei 12.527/2011 (Lei de Acesso à Informação). Sendo assim, realiza o tratamento

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

de dados para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais e cumprir as atribuições legais do serviço público, e, portanto, eventuais dados pessoais dos sócios, representantes legais, prepostos e demais envolvidos na relação do objeto do presente contrato, estarão disponíveis no Portal da Transparência, nos termos do art. 23 da LGPD.

9.3. A CONTRATADA no ato da assinatura do presente instrumento, declara que se encontra adequada e capaz de garantir a devida proteção e manuseio dos dados pessoais que sejam tangíveis, ou que, pessoalmente identifiquem ou tornem identificáveis, quaisquer empregados, clientes, agentes, usuários final, fornecedor, contatos, ou qualquer pessoa natural cujos dados pessoais sejam objeto de tratamento das respectivas instituições a quem pertencem os sócios quotistas incluindo suas filiais, subsidiárias, ou grupo econômico a que pertençam, em conformidade com a LGPD.

9.4. O tratamento de dados pessoais dar-se-á de acordo com as bases legais previstas nas hipóteses dos arts. 7º e/ou 11 da Lei 13.709/2018 às quais se submeterão os serviços, e para propósitos legítimos, específicos, explícitos e informados ao titular.

9.5. As partes deverão adotar todas as políticas e medidas protetivas definitivas na LGPD, promovendo políticas de proteção de dados com adoção de ferramentas tecnológicas, jurídicas e humanas, para coleta e proteção de dados pessoais de pessoas naturais, no âmbito do desenvolvimento do objeto do presente contrato.

9.6. Ressalvado o disposto no item 9.7, é vedada à CONTRATADA a subcontratação do processamento dos dados pessoais recebidos, bem como a transferência do processamento ou tratamento para qualquer empresa ou terceiro, inclusive no exterior, sem o consentimento prévio por escrito do CONTRATANTE, no âmbito do objeto deste contrato.

9.7. A CONTRATADA, no âmbito de suas relações comerciais próprias, poderá contratar serviços de armazenamento em nuvem para os dados relacionados ao presente contrato, desde que essenciais à execução dos serviços e em acordo com as finalidades e os limites deste ajuste e as disposições da Lei n.º 13.709/2018 (LGPD).

9.7.1. A CONTRATADA atesta que a prestadora dos serviços de armazenamento em nuvem possui condições de fornecer o nível adequado de proteção dos dados sob a sua guarda, em conformidade com as exigências estipuladas na Lei n.º 13.709/2018 (LGPD).

9.7.2. A prestadora dos serviços de armazenamento em nuvem atuará na condição de suboperadora dos dados e, no caso de descumprir as determinações da Lei n.º 13.709/2018 (LGPD), responderá a CONTRATADA perante o CRCMG.

9.8. A CONTRATADA se compromete a, na execução das suas atividades contratualmente previstas, não coletar dados pessoais de terceiros sem a observância dos pressupostos da LGPD, tampouco compartilhar ou enviar tais dados para a CONTRATANTE, quando seu tratamento estiver em desconformidade com a referida legislação, sob pena de caracterizar inadimplemento contratual, passível, inclusive, de motivar a rescisão prevista no presente instrumento.

9.9. Os dados obtidos em razão desse contrato serão armazenados em um banco de dados seguro, com garantia de registro das transações realizadas na aplicação de acesso (log) e adequado controle de acesso baseado em

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

função (*role based access control*) e com transparente identificação do perfil dos credenciados, tudo estabelecido como forma de garantir inclusive a rastreabilidade de cada transação e a franca apuração, a qualquer momento, de desvios e falhas, vedado o compartilhamento desses dados com terceiros;

9.10. A CONTRATADA se compromete com a qualidade dos dados pessoais eventualmente fornecidos à CONTRATANTE em decorrência do presente contrato, zelando pela entrega de dados corretos e atualizados, buscando sempre o melhor interesse dos titulares, respeitando os seus direitos e reforçando sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, nos termos do artigo 23 da LGPD.

9.11. Encerrada a vigência do contrato ou não havendo mais necessidade de utilização dos dados pessoais, sejam eles sensíveis ou não, a CONTRATADA interromperá o tratamento dos dados pessoais, e os eliminará completamente com todas as cópias porventura existentes (seja em formato digital ou físico), no prazo máximo de 30 (trinta) dias, salvo quando a CONTRATADA tenha que mantê-los para cumprimento de obrigação legal ou outra hipótese da LGPD, sob pena de responsabilização administrativa, cível e penal.

9.12. Em caso de eventual coleta de dados pessoais sensível, esta será realizada mediante prévia aprovação do CONTRATANTE, responsabilizando-se a CONTRATADA por obter o consentimento dos titulares (salvo nos casos em que opere outra hipótese legal de tratamento). Os dados assim coletados só poderão ser utilizados na execução dos serviços especificados neste contrato, e em hipótese alguma poderão ser compartilhados ou utilizados para outros fins.

9.13. Eventualmente, as partes podem ajustar que o CONTRATANTE será responsável por obter o consentimento dos titulares, observadas as demais condicionantes no item 9.11 acima.

9.14. As partes informarão imediatamente entre si caso o titular dos dados, a Autoridade Nacional de Proteção de Dados (ANPD) ou terceiros solicitem informações sobre o tratamento de dados pessoais relacionados ao presente contrato ou mesmo determine, legalmente amparada, a eliminação ou anonimização dos dados compartilhados.

9.15. A CONTRATADA cooperará com o CONTRATANTE no cumprimento das obrigações referentes ao exercício dos direitos dos titulares previstos na LGPD e nas Leis e Regulamentos de Proteção de Dados em vigor e, também, no atendimento de requisições e determinações do Poder Judiciário, Ministério Público e órgãos de controle externo.

10. CLÁUSULA DÉCIMA - DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO CRCMG

10.1. A CONTRATADA deverá tomar conhecimento da Política de Segurança da Informação do CRCMG, instituída pela Resolução CRCMG nº 441/2021, disponível em <http://cadastro.crcmg.org.br/ged/>, e se comprometer com a observância e o acatamento de suas diretrizes, sempre que tiver acesso a qualquer informação ou comunicação do CRCMG, oriundas da relação firmada por este instrumento.

CLÁUSULA DÉCIMA PRIMEIRA – DA ASSINATURA ELETRÔNICA/DIGITAL

11.1. Nos termos da Lei nº 14.063/2020 e do Decreto nº 10.543/2020, as partes e as testemunhas concordam expressamente em utilizar assinatura eletrônica para ratificação e legitimação dos termos ajustados no presente instrumento, reconhecendo que a formalização, por esse procedimento, é bastante suficiente à sua integral validade jurídica e vinculação das partes ao Contrato.



Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

11.2. As partes renunciam à possibilidade de exigir a troca, envio ou entrega das vias originais (não eletrônicas) assinadas do instrumento, bem como renunciam ao direito de recusar ou contestar a validade das assinaturas digitais ou eletrônicas, na medida máxima permitida pela legislação aplicável.

CLÁUSULA DÉCIMA SEGUNDA - DO FORO

12.1. Fica eleito o foro da Justiça Federal - Subseção de Belo Horizonte, para dirimir as questões oriundas deste contrato, com renúncia de qualquer outro por mais privilegiado que seja.

E por estarem as partes justas e contratadas, assinam o presente instrumento em 02 (duas) vias de igual teor, para um só efeito.

Considera-se o contrato celebrado na data em que o último representante legal das partes, neste instrumento, assinou.

Belo Horizonte,

CONSELHO REGIONAL DE CONTABILIDADE DE MINAS GERAIS
Contador XXXXXXXX

EMPRESA XXXX
XXXXXXXXX – XXXXXXXX

Testemunhas

Assinatura:

Assinatura:

CPF:

CPF:

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

ANEXO IV - CATÁLOGO DE SERVIÇO

Serviço de monitoramento de ataques cibernéticos e resposta a incidentes		
Item	Descrição	Prioridade
Customização de Regras	Customização de 2 (dois) casos de uso por ano	P7
Criação de Conectores	Criação de 1 (um) conector por ano	P8
Monitoramento de Ataques Cibernéticos	Eventos de Informação	P4
	Eventos de Aviso	P3
	Eventos de Exceção	P2
Resposta a Incidentes de Segurança	Apoio a Resposta de Incidente Crítico - Sistema totalmente inoperante com impacto nas operações críticas de negócio	P1
	Apoio à Resposta de Incidente Alto - Sistema parcialmente inoperante com impacto nas operações críticas de negócio	P2
	Apoio à Resposta de Incidente Médio - Sistema parcialmente inoperante sem impacto nas operações críticas de negócio	P3
	Apoio à Resposta de Incidente Baixo - Informacional, ajustes na configuração, dúvidas e/ou esclarecimentos	P4
Plano de Resposta a Incidentes	Apoio na Elaboração do Plano de Resposta	P7

Tabela 2- Serviços de monitoramento de ataques cibernéticos e resposta a incidentes

Serviço de Gestão de Vulnerabilidades		
Item	Descrição	Prioridade
Varreduras de vulnerabilidade	Checagem (Scan) e varredura Diária	P4
	Checagem (Scan) e varredura Semanal	P7
	Checagem (Scan) e varredura Mensal	P8
Elaboração de Relatórios	Report Executivo Mensal de vulnerabilidades com base em Vetores de Ataque	P8
	Reports automatizados e SMS para cada Scanner Executado	P4
	Report Mensal de ações executadas no processo de gestão de vulnerabilidades	P8
Reuniões	Reunião Mensal de Apresentação dos Reports	P8
	Reunião Mensal de Priorização de ativos e reavaliação da estrutura	P8

Tabela 3- Serviço de Gestão de Vulnerabilidades

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

Serviço de monitoramento, detecção e resposta a incidentes para Endpoints		
Item	Descrição	Prioridade
Operação Reativa	Heath Check - Padronizado	P7
	Relatório de Resumo Mensal de Serviços	P8
Operação Proativa	Notificação de Vulnerabilidades em aplicações e S.O.s	P4
	Reuniões periódicas com proposta de melhoria e evolução da maturidade	P8
	Relatórios customizados	P8
Customização	Criação, Alteração ou Remoção de política de segurança específica	P5
Consulta Informacional	Requisição de suporte para sanar dúvidas	P6
Ativação	Requisição de suporte para ativação de agente	P6
Suspeita de Ameaça	Requisição de suporte para análise de suspeita de anomalia	P5
Impacto no Ambiente	Requisição de suporte para correção de impacto	P4
Parada do Ambiente	Requisição de suporte para restauração do ambiente	P3

Tabela 4- Serviço de monitoramento, detecção e resposta a incidentes para Endpoints



Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

ANEXO V – ATESTADO DE VISTORIA

Atestamos que a empresa xxxxxxxxxxxxxxxxxxxxxxxx, inscrita no CNPJ sob nº xxxxxxxxxxxxxxxxxxxxxxxx, representada pelo(a) Sr(a). xxxxxxxxxxxxxxxxxxxxxxxx, portador(a) do CPF nº xxxxxxxxxxxxxxxxxxxxxxxx e RG nº xxxxxxxxxxxxxxxxxxxxxxxx, visando à formalização de proposta relativa ao Pregão Eletrônico nº 0xx/2023, cujo objeto é a contratação de empresa especializada em SERVIÇOS GERENCIADOS DE SEGURANÇA, **REALIZOU VISTORIA** na sede do Conselho Regional de Contabilidade de Minas Gerais (CRCMG), localizada na rua Cláudio Manoel, nº 639, bairro Savassi, Belo Horizonte-MG, local onde os serviços serão prestados, tomando conhecimento das condições, das especificações, da estrutura local, assim como das demais peculiaridades e especificidades inerentes à execução do serviços objeto da contratação, assumindo, dessa forma, todos os riscos e consequências relativos à prestação integral dos serviços, isentando o CRCMG de qualquer ônus futuro por incompatibilidade dos seus custos decorrentes do adimplemento do objeto.

O representante da empresa, para comprovação de sua condição, deverá apresentar:

- Documento de identificação;
- Carta de apresentação devidamente assinada por quem de direito.

Belo Horizonte, XX de XXXX de 2023.

Representante do CRCMG

Recebido:



Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

ANEXO VI – DECLARAÇÃO DE CIÊNCIA DAS INFORMAÇÕES E CONDIÇÕES DE EXECUÇÃO DOS SERVIÇOS

[EM PAPEL TIMBRADO DA EMPRESA]

A empresa [NOME DA EMPRESA],, com sede no endereço: [ENDEREÇO DA EMPRESA],, inscrita no CNPJ sob o nº [CNPJ DA EMPRESA],, por meio de seu representante legal, Sr(a) [NOME DO REPRESENTANTE DA EMPRESA], portador do CPF nº [CPF DO REPRESENTANTE DA EMPRESA], e RG nº [RG DO REPRESENTANTE DA EMPRESA], para fins de participação no Pregão Eletrônico nº 0xx/2023, cujo objeto é a contratação de empresa especializada em SERVIÇOS GERENCIADOS DE SEGURANÇA, a serem executados na sede do CRCMG, localizada na rua Cláudio Manoel, nº 639, bairro Savassi, Belo Horizonte-MG, durante o período de 12 (doze) meses, **DECLARA** ter pleno conhecimento das condições, das especificações, da estrutura local, assim como das demais peculiaridades e especificidades inerentes à execução dos serviços objeto da contratação, assumindo, dessa forma, todos os riscos e consequências relativos à prestação integral dos serviços, isentando o CRCMG de qualquer ônus futuro por incompatibilidade dos seus custos decorrentes do adimplemento do objeto.

Belo Horizonte, ____ de _____ de 2023.

Assinatura do representante da empresa

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

ANEXO VII - DECLARAÇÃO FORMAL DE DISPONIBILIDADE TÉCNICA
QUALIFICAÇÃO TÉCNICA DOS PROFISSIONAIS DA EMPRESA

Eu, [NOME DA PESSOA], pessoa física com residência em [ENDEREÇO DA PESSOA], inscrita no CPF com o n.º [N.º DO CPF], [E-MAIL], atesto, na condição de seu representante, que a empresa [NOME DA EMPRESA], [ENDEREÇO DA EMPRESA], [CNPJ DA EMPRESA], possui, em seus quadros, profissionais com as qualificações técnicas, em conformidade com os requisitos estabelecidos no Termo de Referência do **Edital 0xx/2023**, atendendo, no mínimo, as seguintes características relativas à formação acadêmica, certificações e experiências:

1. Qualificações técnicas do **GERENTE DE PROJETO**:

Certificações	Descrição
Ao menos uma das certificações de segurança da informação: • Project Management Professional (PMP); • Prince2 Practitioner Certificate in Project Management; • Professional Scrum Master I;	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em gerência de projetos, com experiência mínima de 12 (doze) anos.

Tabela 1 - Qualificações Gerente de Projeto

2. Qualificações técnicas **PREPOSTO**:

Certificações	Descrição
Ao menos uma das certificações de segurança da informação: • CISSP (Certified Information Systems Security Professional); • CISM (Certified Information Security Manager); • CIA (Certified Intrusion Analyst); • GSEC (GIAC Security Essentials); • GCIH (GIAC Incident Handler); • GMON (GIAC Continuous Monitoring);	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência mínima de 5 (cinco) anos em coordenação e gestão de contratos de serviços continuados.

Tabela 2 - Qualificações do Preposto

3. Qualificações técnicas do(s) **analista(s)** que participará do **GRUPO DE ATAQUE CIBERNÉTICO CONTROLADO (Red Team)**:

Certificações	Descrição
• CompTIA Security+ • CompTIA CySA+	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

e/ou Certified Ethical Hacker Certificação em pelo menos uma das soluções escolhidas para atender o tópico SOBRE AS FERRAMENTAS A SEREM UTILIZADAS	graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.

Tabela 3 - Qualificações Grupo de Ataque Cibernético Controlado (Red Team)

4. As qualificações técnicas do(s) **analista(s)** que participará do **GRUPO DE MONITORAMENTO DE ATAQUES**:

Certificações	Descrição
- CompTIA Security+ e/ou - CompTIA CySA+ e/ou - Certified Ethical Hacker	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de SIEM e ATD. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.

Tabela 4 - Qualificações Grupo de Monitoramento de Ataques

5. As qualificações técnicas do(s) **analista(s)** que participará do **GRUPO DE RESPOSTA A INCIDENTE DE SEGURANÇA (CSIRT – Blue Team)**:

Certificações	Descrição
- CompTIA Security+ - CompTIA CySA+ - Certified Ethical Hacker - CompTIA Pentest+ ou - Computer Hacking Forensic Investigator	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC);

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

	Especializações na área de segurança da informação. Conhecimento avançado em segurança da informação, com experiência em resposta a incidente de segurança da informação. Experiência comprovada de no mínimo 5 (cinco) anos em segurança da informação.

Tabela 5 - Qualificações Grupo de Resposta a Incidente de Segurança (CSIRT – *Blue Team*)

Observações:

As certificações e os conhecimentos e experiências dos profissionais deverão atender aos requisitos mínimos estabelecidos no Termo de Referência, conforme modelo de declaração constante deste Anexo, para cada profissional, de acordo com sua área de atuação, sob pena de desclassificação da licitante.

No momento da assinatura do contrato, a empresa deverá comprovar o vínculo com os referidos profissionais, apresentando cópia da Carteira de Trabalho e Previdência Social (CTPS), no caso de haver relação de emprego, ou de contrato de prestação de serviços, regidos pela legislação civil.

Em todo caso, os profissionais deverão estar disponíveis à prestação dos serviços de modo permanente, durante toda a vigência contratual.

Não serão aceitos vínculos de natureza eventual ou precária, inclusive os decorrentes de terceirização ou subcontratação.

Belo Horizonte, ____ de _____ de 2023.

 Assinatura do representante da empresa

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

ANEXO VIII - MODELO DE TERMO DE CONFIDENCIALIDADE E SIGILO DO PRESTADOR

A CONTRATADA deverá assinar termo de sigilo e confidencialidade conforme modelo abaixo:

TERMO DE CONFIDENCIALIDADE E SIGILO DO PRESTADOR

Eu, [NOME DA PESSOA], pessoa física com residência em [ENDEREÇO DA PESSOA], inscrita no CPF com o n.º [N.º DO CPF], [E-MAIL], atesto, na condição de seu representante, que a empresa [NOME DA EMPRESA], [ENDEREÇO DA EMPRESA], [CNPJ DA EMPRESA], doravante denominado simplesmente signatário, por tomar conhecimento de informações sobre o ambiente computacional do Conselho Regional de Contabilidade de Minas Gerais, aceita as regras, condições e obrigações seguintes:

1. A não utilizar QUAISQUER informações (Técnicas Administrativas ou Gerenciais), confidenciais ou não, a que tiver acesso, para gerar benefício próprio exclusivo e/ou unilateral, presente ou futuro, ou para o uso de terceiros;
2. A não efetuar nenhuma gravação ou cópia da documentação a que tiver acesso;
3. A não apropriar para mim ou para outrem de QUALQUER material técnico, gerencial ou administrativo que venha a ser disponível;
4. A não repassar o conhecimento das informações, responsabilizando-se por todas as pessoas que vierem a ter acesso às informações, por seu intermédio, e obrigando-se, assim, a ressarcir a ocorrência de qualquer dano e/ou prejuízo oriundo de uma eventual quebra de sigilo ou confidencialidade de todas as informações fornecidas;
5. Em cuidar para que as informações confidenciais fiquem restritas ao conhecimento tão somente das pessoas que estejam diretamente envolvidas nas discussões, análises, reuniões e negócios, devendo cientificá-las da existência deste Termo e da natureza confidencial destas informações.

Neste Termo, as seguintes expressões serão assim definidas:

Informação Confidencial significará toda informação revelada por meio do manual de serviço, excetuando-se deste os níveis permitidos pelo fabricante para os quais o CRCMG tenha sido treinado.

Informação inclui, mas não se limita, à informação relativa às documentações técnicas, relatórios técnicos, operações, instalações, equipamentos, segredos de negócio, segredo de fábrica, dados, habilidades especializadas, projetos, métodos e metodologia, sistemas, softwares, bases de dados, fluxogramas, especializações, componentes, fórmulas, produtos, amostras, diagramas, desenhos de esquema industrial, patentes, oportunidades de mercado e questões relativas a negócios revelados nos manuais de serviço. Não constituirá "Informação" ou "Informação Confidencial" para os propósitos deste Termo aquela que:

- a) Seja de domínio público no momento da revelação ou após a revelação, exceto se isso ocorrer em decorrência de ato ou omissão da Parte Receptora;
- b) Já esteja em poder da Parte Receptora, como resultado de sua própria pesquisa, contanto que a Parte Receptora possa comprovar esse fato;



Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	0XX/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	0XX/2023

- c) Tenha sido legitimamente recebida de terceiros;
- d) Seja revelada em razão de uma ordem válida ou de uma ordem judicial, somente até a extensão de tais ordens, contanto que a Parte Receptora tenha notificado a existência de tal ordem, previamente e por escrito, à Parte Reveladora, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis;
- e) Tenham sido objeto de treinamento dos profissionais do CRCMG.

A vigência da obrigação de confidencialidade e sigilo, assumida pela minha pessoa por meio deste termo, terá a validade enquanto a informação não for tornada de conhecimento público por qualquer outra pessoa, ou mediante autorização escrita, concedida à minha pessoa pelas partes interessadas neste termo. Pelo não cumprimento do presente Termo de Confidencialidade e Sigilo, fica o abaixo assinado ciente de todas as sanções judiciais que poderão advir.

Belo Horizonte, ____ de _____ de 2023.

Assinatura do representante da empresa
(Mesmo signatário do contrato)

	DESPACHO DE PROCESSO PARA A ASSESSORIA JURÍDICA

NÚMERO DO PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
NÚMERO DO PROCESSO E MODALIDADE	Pregão Eletrônico nº 001/2023
OBJETO	Contratação de empresa especializada em SERVIÇOS GERENCIADOS DE SEGURANÇA.

À
Assessoria Jurídica do CRCMG

Sr. Assessor,

Encaminhamos o presente processo para análise e emissão de parecer.

Belo Horizonte, 23 de janeiro de 2023.

Assinado digitalmente por:
ANDREZA MAIA BITARAES
CPF: 045.174.336-92
Certificado emitido por AC CERTIFICA MINAS v5
Data: 23/01/2023 15:04:58 -03:00



Andreza Maia Bitarães
Assistente
Gerência Administrativa e Financeira

PE-002/AF
4/10/2018



MANIFESTO DE ASSINATURAS



Código de validação: BKKNG-PW9PF-RZ6VX-8ZT8G

Esse documento foi assinado pelos seguintes signatários nas datas indicadas (Fuso horário de Brasília):

- ✓ ANDREZA MAIA BITARAES (CPF 045.174.336-92) em 23/01/2023 15:04 -
Assinado com certificado digital ICP-Brasil

Para verificar as assinaturas, acesse o link direto de validação deste documento:

<https://assinador.crcmg.org.br/validate/BKKNG-PW9PF-RZ6VX-8ZT8G>

Ou acesse a consulta de documentos assinados disponível no link abaixo e informe o código de validação:

<https://assinador.crcmg.org.br/validate>

PARECER JURÍDICO

REFERÊNCIA: PAC Nº 016/2023

Relatório

Na data de 23 de janeiro de 2023, foi encaminhado Processo Administrativo de Contratação nº 016/2023 - Pregão Eletrônico 01/2023 pela Gerência Administrativa e Financeira (fls. 400 a 401), em que se solicitou manifestação desta Assessoria Jurídica sobre contratação de empresa especializada em SERVIÇOS GERENCIADOS DE SEGURANÇA.

Fundamentação

Na documentação que instrui o processo (PAC Nº 016/2023 – numerado de 01 a 401), em “Formalização da Demanda” o setor requisitante, Gerência de Tecnologia da Informação, apresentou justificativa da necessidade dos bens descritos acima, conforme (fls. 02 a 04):

“Em decorrência dos constantes ataques cibernéticos a diversas instituições públicas e privadas e da implantação da LGPD no CRCMG, que exige a adoção de medidas de segurança, torna-se indispensável a aplicação de boas práticas de segurança da informação no ambiente tecnológico do CRCMG.

Diante do crescimento exponencial de ameaças e ataques sofridos a empresas privadas e órgãos públicos no Brasil e no mundo, investimentos contínuos em segurança da informação são fundamentais para a mitigação de riscos de segurança associados ao negócio de maneira a resguardar a confidencialidade, a disponibilidade e a integridade das informações.

O cenário de ameaças à segurança da informação não se resume a ataques aos serviços de TI pela Internet. Tentativas de acesso não autorizadas, infecção por arquivos maliciosos (vírus), e-mails indesejados (SPAMs), engenharia social, entre outros, são exemplos de eventos que podem apresentar riscos à segurança de TI. Até mesmo colaboradores não conscientes ou mal-intencionados representam risco potencial à segurança da informação.

O Conselho Regional de Contabilidade de Minas Gerais vem utilizando, cada vez mais, soluções de TI na busca de aperfeiçoamento da sua missão institucional e gestão pública. Junto a isso, vem também disponibilizando aos seus colaboradores,

aos profissionais contábeis e à sociedade diversos serviços de TI. Nesse cenário, diversas foram as mudanças: tanto em termos de quantidade de serviços oferecidos quanto a diversidade de soluções. Conforme cresce a oferta de serviços aumentam-se os riscos relacionados e a necessidade de monitoramento.

Nesse sentido, incidentes de segurança da informação, como nas hipóteses de violação, roubo ou perda de informações custodiadas pelo CRCMG, podem constituir possíveis situações capazes de inviabilizar, senão a totalidade, parte das atividades desta entidade. Assim, a ocorrência de eventuais sinistros poderia provocar o vazamento de informações, prejuízo à sua imagem, podendo ainda a entidade que responder pelos danos causados.

Como o CRCMG não dispõe de funcionários em seu quadro de empregados nem cargo em seu plano de cargos e salários para atender à demanda com elevado nível de conhecimento que o ambiente exige, considera-se necessária a contratação de empresa especializada para esta finalidade, que forneça pessoal especializado em segurança da informação que propicie a integridade, a confidencialidade, a autenticidade e a disponibilidade dos dados, através de um monitoramento preventivo e contínuo de segurança da informação contra ataques cibernéticos e de serviço de resposta a incidentes de segurança.

A contratação pretendida está alinhada com o planejamento estratégico do CRCMG, uma vez que contribuirá para o alcance do objetivo da qualidade de “assegurar meios e recursos que possibilitem o cumprimento das políticas e diretrizes da gestão”, bem como dos objetivos estratégicos de “garantir qualidade e confiabilidade nos processos e nos procedimentos”.

O documento mencionado acima contou com o “De acordo” da Diretoria Executiva, através de Mário Rogério Marotta.

Constaram também no processo em tela Estudos Técnicos Preliminares elaborados pela Equipe de Planejamento (fls. 05 a 17) – em que a mesma afirmou *“Diante dos elementos consignados neste estudo, foi possível constatar que o objeto da contratação em epígrafe está alinhado com o Planejamento Estratégico do CRCMG e com o interesse público, que há recursos orçamentários suficientes à cobertura das despesas correspondentes, tendo em vista a previsibilidade da contratação no Plano de Trabalho, PDTI e Plano Anual de Contratações do CRCMG, e que a solução escolhida está de acordo com a prática de mercado, havendo fornecedores qualificados para prestar os serviços na forma pretendida. Assim, a equipe de planejamento declara que a contratação, objeto deste estudo, é viável sob os aspectos econômicos, de conveniência e oportunidade.”*, acompanhados por Mapa de Riscos (fls. 18 a 21).

Ainda presente Termo de Referência (fls. 22 a 113) - também assinado pela Presidente Suely Maria Marques de Oliveira, em que no item 20 (fl. 103), optou-se pela modalidade licitatória pregão em sua forma eletrônica, utilizado para aquisição de bens e serviços comuns, vez que os padrões de desempenho e qualidade podem ser objetivamente definidos pela minuta de edital, por meio de especificações usuais no mercado.

Além disso, faz parte dos autos pesquisa de preços (fls. 114 a 252), parâmetros utilizados para a formação da planilha de composição do preço de referência (fls. 253 a 254), com reserva orçamentária realizada em (fls. 255 e 256).

Autorizada a abertura de processo de contratação pela Presidente da entidade (fls. 257 a 259), destaca-se o seguinte trecho da justificativa:

“(…)

Por esses motivos, e devido ao incidente ocorrido recentemente no ambiente, tendo em vista que o Conselho não dispõe de infraestrutura física e pessoal para o monitoramento e gerenciamento de dispositivos de segurança com diversos fornecedores (firewall, sistema de prevenção de intrusões de rede, gerenciamento unificado de ameaças), capazes de realizar ações contra incidentes de segurança de forma tempestiva e procedimental, torna-se necessária realizar a contratação de uma solução que forneça uma estrutura em segurança da informação adequada, de forma a propiciar a integridade, confidencialidade, autenticidade e a disponibilidade dos dados, através de um monitoramento preventivo e contínuo de segurança da informação contra ataques cibernéticos e de serviço de resposta a incidentes de segurança.

(…)”

Por fim, consta nos processo de contratação administrativa Minuta de Edital (fls. 265 a 399) e despacho de encaminhamento à Assessoria Jurídica (fls. 400 a 401).

É sabido que cabe à Assessoria Jurídica prestar consultoria sob o prisma estritamente jurídico, sem adentrar em aspectos relativos à conveniência e oportunidade dos atos praticados e de natureza eminentemente técnico-administrativa. Assim, compreende-se que as especificações técnicas contidas no presente processo, inclusive o detalhamento do objeto da contratação, características, quantidades, requisitos e especificações, bem como a pesquisa de preços, tenham sido regularmente apurados pela

área técnica do órgão competente e conferidos pela autoridade responsável pela contratação.

Diante dos documentos que compõe o processo de contratação, verifica-se que os trâmites administrativos e legais foram seguidos, mostrando-se a modalidade licitatória apontada apropriada para a contratação dos serviços indicados, em alinhamento com os termos Lei nº 10.520/2002, Decreto 10.024/2019 e Lei nº 8.666/93, sendo o pregão capaz de resguardar o atendimento aos princípios constitucionais, assegurando a proposta mais vantajosa e garantindo a isonomia entre os futuros participantes.

Conclusão

Diante do exposto, resta-nos concluir que a modalidade de licitação pretendida e a possível contratação têm previsão normativa e o processo em curso cumpre os requisitos legais, estando, contudo, a avaliação da conveniência e oportunidade da contratação (que são princípios basilares de Direito Administrativo) dentro da discricionariedade outorgada à Presidente do CRCMG, que, nesta qualidade, deverá decidir a questão.

s.m.j., esse é o parecer.

Belo Horizonte, 23 de janeiro de 2023

Assinado digitalmente por:
WILLIAN FERNANDO DE FREITAS
CPF: 654.085.786-15
Certificado emitido por AC SAFEWEB RFB v5
Data: 23/01/2023 15:54:38 -03:00



Willian Fernando de Freitas
Assessor Jurídico



MANIFESTO DE ASSINATURAS



Código de validação: PQQRW-VTMLV-B797U-P5RRN

Esse documento foi assinado pelos seguintes signatários nas datas indicadas (Fuso horário de Brasília):

- ✓ WILLIAN FERNANDO DE FREITAS (CPF 654.085.786-15) em 23/01/2023
15:54 - Assinado com certificado digital ICP-Brasil

Para verificar as assinaturas, acesse o link direto de validação deste documento:

<https://assinador.crcmg.org.br/validate/PQQRW-VTMLV-B797U-P5RRN>

Ou acesse a consulta de documentos assinados disponível no link abaixo e informe o código de validação:

<https://assinador.crcmg.org.br/validate>

MAPA DE RISCOS											
Objeto		Contratação de serviços de monitoramento preventivo e contínuo de segurança da informação contra ataques cibernéticos e serviço de resposta a incidentes de segurança.									
Equipe de Planejamento		Cláudio Márcio Araújo da Silva Henry Caetano Ávila de Andrade Izaías Angelo Gomes									
FASE DA ANÁLISE											
() Planejamento da contratação (X) Seleção do fornecedor () Execução do Contrato											
Nº	Risco	Consequência	Tipo	Avaliação				Estratégia para eliminar ou minimizar a ocorrência do risco		Estratégia de contingência caso o risco se concretize	
				SEVERIDADE	ABRANGÊNCIA	FREQUENCIA	CLASSE	Ação	Responsável	Ação	Responsável
1	Interposição de recursos.	Retardamento na conclusão da licitação, atraso no início da execução dos serviços.	Externo	2	1	2	4	Conduzir o pregão com diligência, observando a legislação vigente.	Pregoeiro	Priorizar a análise das impugnações e dos recursos recebidos para manifestação das respostas em tempo hábil.	Pregoeiro / Getin / Presidência
2	Falha no julgamento dos documentos de habilitação, qualificação técnica e propostas das licitantes.	Anulação do processo licitatório	Interna	3	1	1	3	Solicitação de auxílio das áreas técnica e jurídica para análise da documentação.	Pregoeiro / Getin / Asjur	Reestabelecimento de fases do processo ou anulação da licitação	Pregoeiro / Presidência

Rua Cláudio Manoel, 639 - Bairro Savassi

Telefone: (31) 3269-8400 – CEP: 30140-105 – Belo Horizonte/MG

 Esse documento foi assinado por IZAIAS ANGELO GOMES, CLAUDIO MARCIO ARAUJO DA SILVA e HENRY CAETANO AVILA DE ANDRADE. Para validar o documento e suas assinaturas acesse <https://assinador.crcmg.org.br/validate/Y2Q5V-PRN5C-NZETH-QWPUW>

A identificação, análise, avaliação e tratamento dos riscos dos processos de contratação do CRCMG são realizados em consonância com o Procedimento Geral PG-007/SQ – Gestão de riscos e oportunidades, considerando que o CRCMG possui uma Política de Gestão de Riscos instituída, conforme Portaria CRCMG nº 132/2017, bem como observando os critérios estabelecidos pela Instrução Normativa SG/MPDG nº 05/2017.

Abrangência:

- 1: Local - Afeta aquele processo especificamente a que está relacionado.
- 2: Adjacente - Afeta mais de um processo.
- 3: Global - Afeta vários processos, internos e externos, impactando o Sistema de Gestão da Qualidade.

Frequência:

- 1: Rara - A ocorrência daquela falha é pequena.
- 2: Eventual - A ocorrência daquela falha é ocasional.
- 3: Frequente - A falha ocorre sempre, por diversas vezes.

Severidade:

- 1: Baixa - Levemente prejudicial. Impactos que não comprometem substancialmente o desenvolvimento do processo.
- 2: Moderada - Prejudicial. Impactos que comprometem o desenvolvimento do processo ou o atendimento aos objetivos.
- 3: Alta - Extremamente prejudicial. Impactos que comprometem substancialmente o desenvolvimento do processo, bem como o atendimento aos objetivos.

Classificação do risco

A classificação do risco consiste na multiplicação dos valores atribuídos aos fatores severidade, abrangência e frequência: $CLASSE = SEVERIDADE \times ABRANGÊNCIA \times FREQUÊNCIA$.

A pontuação mínima possível a um determinado impacto é 1 (1 x 1 x 1), indicando que o aspecto não provoca qualquer efeito adverso. A pontuação máxima possível é 27 (3 x 3 x 3), o que significa que o aspecto é extremamente prejudicial.

A classificação do impacto em ser ou não significativo obedece ao agrupamento definido abaixo:

- Resultado de 1 a 4: Risco tolerável.
 Resultado de 6 a 12: Risco moderado.
 Resultado de 18 a 27: Risco crítico.

Os riscos externos e os riscos internos classificados como toleráveis não requerem uma ação específica de tratamento, devendo ser monitorados.

Rua Cláudio Manoel, 639 - Bairro Savassi
 Telefone: (31) 3269-8400 – CEP: 30140-105 – Belo Horizonte/MG
 crcmg@crcmg.org.br – www.crcmg.org.br

Cabe à Comissão de Governança, Riscos e Compliance realizar a priorização dos riscos classificados como críticos e moderados, classificando aqueles que são considerados riscos-chave e avaliando a necessidade de abertura de plano de ação, e levar à aprovação do Conselho Diretor.

Tratamento do risco:

O tratamento de riscos envolve a seleção de uma ou mais opções para modificar os riscos e a implementação dessas opções, que podem ser, entre outras:

- a) aceitar o risco;
- b) transferir ou compartilhar o risco com outra parte;
- c) evitar o risco pela decisão de descontinuar ou não iniciar a atividade;
- d) abrir plano de ação para mitigar ou reduzir o risco.

Assinado digitalmente por:
CLAUDIO MARCIO ARAUJO DA SILVA
CPF: 691.116.426-53
Certificado emitido por AC SOLUTI Multipla
Data: 19/01/2023 11:00:28 -03:00



Cláudio Márcio Araújo da Silva
Membro

Assinado digitalmente por:
HENRY CAETANO AVILA DE ANDRADE
CPF: 059.963.316-67
Certificado emitido por AC VALID RFB v5
Data: 19/01/2023 14:00:03 -03:00



Henry Caetano Ávila de Andrade
Membro

Assinado digitalmente por:
IZAIAS ANGELO GOMES
CPF: 046.926.156-05
Certificado emitido por AC SOLUTI Multipla v5
Data: 19/01/2023 09:32:21 -03:00



Izaías Angelo Gomes
Membro

Rua Cláudio Manoel, 639 - Bairro Savassi
Telefone: (31) 3269-8400 – CEP: 30140-105 – Belo Horizonte/MG
crcmg@crcmg.org.br – www.crcmg.org.br

Esse documento foi assinado por IZAIAS ANGELO GOMES, CLAUDIO MARCIO ARAUJO DA SILVA e HENRY CAETANO AVILA DE ANDRADE. Para validar o documento e suas assinaturas acesse <https://assinador.crcmg.org.br/validate/Y2Q5V-PRN5C-NZETH-QWPUW>



MANIFESTO DE ASSINATURAS



Código de validação: Y2Q5V-PRN5C-NZETH-QWPUW

Esse documento foi assinado pelos seguintes signatários nas datas indicadas (Fuso horário de Brasília):

- ✓ IZAIAS ANGELO GOMES (CPF 046.926.156-05) em 19/01/2023 09:32 -
Assinado com certificado digital ICP-Brasil
- ✓ CLAUDIO MARCIO ARAUJO DA SILVA (CPF 691.116.426-53) em 19/01/2023
11:00 - Assinado com certificado digital ICP-Brasil
- ✓ HENRY CAETANO AVILA DE ANDRADE (CPF 059.963.316-67) em 19/01/2023
14:00 - Assinado com certificado digital ICP-Brasil

Para verificar as assinaturas, acesse o link direto de validação deste documento:

<https://assinador.crcmg.org.br/validate/Y2Q5V-PRN5C-NZETH-QWPUW>

Ou acesse a consulta de documentos assinados disponível no link abaixo e informe o código de validação:

<https://assinador.crcmg.org.br/validate>

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

EDITAL

O **CONSELHO REGIONAL DE CONTABILIDADE DE MINAS GERAIS**, Autarquia Federal criada pelo Decreto-Lei nº 9.295/46, CNPJ: 17.188.574/0001-38, torna público, para ciência dos interessados, que por intermédio de seu Pregoeiro, designado pela Portaria CRCMG nº 117/2020, realizará licitação na modalidade **PREGÃO, na forma ELETRÔNICA**, do tipo **MENOR PREÇO**. O procedimento licitatório observará integralmente as disposições da Lei nº 10.520/2002, da Lei nº 13.709/2018, dos Decretos nº 3.555/2000, nº 7.746/2012, nº 8.538/2015, nº 9.178/2017, nº 9.507/2018 e nº 10.024/2019; da Lei Complementar nº 123/2006, alterada pelas Leis Complementares nº 155/2016 e nº 147/2014, das Instruções Normativas SEGES/MP nº 5/2017 e SEGES/MP nº 3/2018; aplicando-se, subsidiariamente, as normas da Lei nº 8.666/93, bem como pelas condições estabelecidas neste Edital.

DA SESSÃO PÚBLICA DO PREGÃO ELETRÔNICO:

A abertura da presente licitação dar-se-á em sessão pública, dirigida pelo Pregoeiro designado, a ser realizada de acordo com a legislação mencionada no preâmbulo deste Edital conforme indicado abaixo:

Data da abertura das propostas: **06/02/2023**

Horário da abertura das propostas: **09h40min**, respeitando o horário de Brasília/DF.

Endereço eletrônico: www.comprasgovernamentais.gov.br

UASG: 925152

1. DO OBJETO

1.1. O objeto da presente licitação é a seleção da proposta mais vantajosa para a contratação de empresa especializada em **SERVIÇOS GERENCIADOS DE SEGURANÇA**, conforme condições e especificações estabelecidas no Anexo I – Termo de Referência deste Edital.

1.2. A licitação será realizada em único item.

1.3. O critério de julgamento adotado será o menor preço do item, observadas as exigências contidas neste Edital e seus Anexos quanto às especificações do objeto.

1.4. Integram este Edital os anexos I, II, III, IV, V, VI, VII e VIII.

2. DOS RECURSOS ORÇAMENTÁRIOS

2.1. As despesas para atender a esta licitação estão programadas em dotação orçamentária própria, prevista no plano de trabalho do CRCMG para o exercício de 2023, conforme indicação abaixo:

Projeto: 5002	Centro de Custo: 327	Conta contábil: 6.3.1.3.02.01.005

3. DO CREDENCIAMENTO

3.1. O Credenciamento é o nível básico do registro cadastral no SICAF, que permite a participação dos interessados na modalidade licitatória Pregão, em sua forma eletrônica.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

3.2. O cadastro no SICAF deverá ser feito no Portal de Compras do Governo Federal, no sítio www.comprasgovernamentais.gov.br, por meio de certificado digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP - Brasil.

3.3. O credenciamento junto ao provedor do sistema implica a responsabilidade do licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes a este Pregão.

3.4. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

3.5. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais no SICAF e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

3.5.1. A não observância do disposto no subitem anterior poderá ensejar desclassificação no momento da habilitação.

4. DA PARTICIPAÇÃO NO PREGÃO

4.1. Poderão participar deste Pregão interessados cujo ramo de atividade seja compatível com o objeto desta licitação, e que estejam com Credenciamento regular no Sistema de Cadastramento Unificado de Fornecedores – SICAF, conforme disposto no art. 9º da IN SEGES/MP nº 3, de 2018.

4.1.1. Os licitantes deverão utilizar o certificado digital para acesso ao Sistema.

4.1.2. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no artigo 34 da Lei nº 11.488, de 2007, para o agricultor familiar, o produtor rural pessoa física e para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006.

4.2. Não poderão participar desta licitação os interessados:

4.2.1. proibidos de participar de licitações e celebrar contratos administrativos, na forma da legislação vigente;

4.2.2. que não atendam às condições deste Edital e seu(s) anexo(s);

4.2.3. estrangeiros que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;

4.2.4. que se enquadrem nas vedações previstas no artigo 9º da Lei nº 8.666, de 1993;

4.2.5. que estejam sob falência, recuperação judicial ou extrajudicial, ou concurso de credores ou insolvência, em processo de dissolução ou liquidação, observado o disposto no item 10.10.1.1 deste Edital;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

4.2.6. entidades empresariais que estejam reunidas em consórcio;

4.2.7. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição (Acórdão nº 746/2014-TCU-Plenário);

4.3. Nos termos do art. 5º do Decreto nº 9.507, de 2018, é vedada a contratação de pessoa jurídica na qual haja administrador ou sócio com poder de direção, familiar de:

4.3.1. detentor de cargo em comissão ou função de confiança que atue na área responsável pela demanda ou contratação;

4.3.2. Para os fins do disposto neste item, considera-se familiar o cônjuge, o companheiro ou o parente em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau (Súmula Vinculante/STF nº 13, art. 5º, inciso V, da Lei nº 12.813, de 16 de maio de 2013 e art. 2º, inciso III, do Decreto nº 7.203, de 04 de junho de 2010);

4.4. Nos termos do art. 7º do Decreto nº 7.203, de 2010, é vedada, ainda, a utilização, na execução dos serviços contratados, de empregado da futura Contratada que seja familiar de agente público ocupante de cargo em comissão ou função de confiança nesta Entidade contratante.

4.5. Como condição para participação no Pregão, o licitante assinalará “sim” ou “não” em campo próprio do sistema eletrônico, relativo às seguintes declarações:

4.5.1. que cumpre os requisitos estabelecidos no artigo 3º da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49.

4.5.1.1. nos itens exclusivos para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame;

4.5.1.2. nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte ou sociedade cooperativa.

4.5.2. que está ciente e concorda com as condições contidas no Edital e seus anexos;

4.5.3. que cumpre os requisitos para a habilitação definidos no Edital e que a proposta apresentada está em conformidade com as exigências editalícias;

4.5.4. que inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores;

4.5.5. que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7º, XXXIII, da Constituição;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

4.5.6. que não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

4.5.7. que os serviços são prestados por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação, conforme disposto no art. 93 da Lei nº 8.213, de 24 de julho de 1991.

4.6. A declaração falsa relativa ao cumprimento de qualquer condição sujeitará o licitante às sanções previstas em lei e neste Edital.

5. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

5.1. Os licitantes encaminharão, exclusivamente por meio do sistema, concomitantemente com os documentos de habilitação exigidos no edital, proposta com a descrição do objeto ofertado e o preço, até a data e o horário estabelecidos para abertura da sessão pública, quando, então, encerrar-se-á automaticamente a etapa de envio dessa documentação.

5.1.1. Os documentos de habilitação a que se refere o item acima são aqueles previstos no **ITEM 10 - DA HABILITAÇÃO** deste Edital.

5.1.2. Será desclassificado o licitante que não inserir no sistema previamente à abertura da sessão pública, a proposta de preços e os documentos de habilitação exigidos no **ITEM 10 - DA HABILITAÇÃO** ou que apresentá-los em desacordo com o estabelecido neste Edital.

5.2. O envio da proposta, acompanhada dos documentos de habilitação exigidos neste Edital, ocorrerá por meio de chave de acesso e senha.

5.3. Os licitantes poderão deixar de apresentar os documentos de habilitação que constem do SICAF, assegurado aos demais licitantes o direito de acesso aos dados constantes dos sistemas.

5.4. As Microempresas e Empresas de Pequeno Porte deverão encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art. 43, § 1º da LC nº 123, de 2006.

5.5. Incumbirá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

5.6. Até a abertura da sessão pública, os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema.

5.7. Não será estabelecida, nessa etapa do certame, ordem de classificação entre as propostas apresentadas, o que somente ocorrerá após a realização dos procedimentos de negociação e julgamento da proposta.

5.8. Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados para avaliação do pregoeiro e para acesso público após o encerramento do envio de lances.

6. DO PREENCHIMENTO DA PROPOSTA

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

6.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

6.1.1. **Valor unitário e total do item;**

6.1.2. Descrição do objeto, contendo as informações similares à especificação do Termo de Referência.

6.2. Todas as especificações do objeto contidas na proposta vinculam a Contratada.

6.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na prestação dos serviços;

6.3.1. A Contratada deverá arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do §1º do artigo 57 da Lei nº 8.666, de 1993.

6.3.2. Caso o eventual equívoco no dimensionamento dos quantitativos se revele superior às necessidades da contratante, a Administração deverá efetuar o pagamento seguindo estritamente as regras contratuais de faturamento dos serviços demandados e executados, concomitantemente com a realização, se necessário e cabível, de adequação contratual do quantitativo necessário, com base na alínea "b" do inciso I do art. 65 da Lei n. 8.666/93 e nos termos do art. 63, §2º da IN SEGES/MP n.5/2017.

6.4. O licitante é o único responsável pela cotação correta dos encargos tributários. Em caso de erro ou cotação incompatível com o regime tributário a que se submete, serão adotadas as orientações a seguir:

6.4.1. cotação de percentual menor que o adequado: o percentual será mantido durante toda a execução contratual;

6.4.2. cotação de percentual maior que o adequado: o excesso será suprimido, unilateralmente, da planilha e haverá glosa, quando do pagamento, e/ou redução, quando da repactuação, para fins de total ressarcimento do débito.

6.5. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses, devendo o licitante ou contratada apresentar ao pregoeiro ou à fiscalização, a qualquer tempo, comprovação da adequação dos recolhimentos, para os fins do previsto no subitem anterior.

6.6. Independentemente do percentual de tributo inserido na planilha, no pagamento dos serviços, serão retidos na fonte os percentuais estabelecidos na legislação vigente.

6.7. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar os serviços nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

6.8. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

6.9. O prazo de validade da proposta não será inferior a 60 (sessenta) dias, a contar da data de sua apresentação.

6.10. Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais, quando participarem de licitações públicas.

6.10.1. O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a responsabilização pelo Tribunal de Contas da União e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

7. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

7.1. A abertura da presente licitação dar-se-á em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

7.2. O Pregoeiro verificará as propostas apresentadas, desclassificando desde logo aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital, contenham vícios insanáveis ou não apresentem as especificações técnicas exigidas no Termo de Referência.

7.2.1. Também será desclassificada a proposta que identifique o licitante.

7.2.2. A desclassificação será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

7.2.3. A não desclassificação da proposta não impede o seu julgamento definitivo em sentido contrário, levado a efeito na fase de aceitação.

7.3. O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.

7.4. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

7.5. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio do sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

7.5.1. O lance deverá ser ofertado pelo **VALOR TOTAL DO ITEM**.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

7.6. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

7.7. O licitante somente poderá oferecer lance de valor inferior ou percentual de desconto superior ao último por ele ofertado e registrado pelo sistema.

7.8. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de 100,00 (cem reais).

7.9. Será adotado para o envio de lances no pregão eletrônico o **modo de disputa “aberto”**, em que os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

7.10. A etapa de lances da sessão pública terá duração de dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.

7.11. A prorrogação automática da etapa de lances, de que trata o item anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

7.12. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente.

7.13. Encerrada a fase competitiva sem que haja a prorrogação automática pelo sistema, poderá o pregoeiro, assessorado pela equipe de apoio, justificadamente, admitir o reinício da sessão pública de lances, em prol da consecução do melhor preço.

7.14. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

7.15. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

7.16. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

7.17. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.

7.18. O Critério de julgamento adotado será o **MENOR PREÇO**, conforme definido neste Edital e seus anexos.

7.19. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

7.20. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da LC nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

7.21. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da proposta ou lance de menor preço serão consideradas empatadas com a primeira colocada.

7.22. A melhor classificada nos termos do item anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

7.23. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

7.24. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

7.25. A ordem de apresentação pelos licitantes é utilizada como um dos critérios de classificação, de maneira que só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

7.25.1. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 3º, § 2º, da Lei nº 8.666, de 1993, assegurando-se a preferência, sucessivamente, aos serviços:

7.25.1.1. produzidos no país;

7.25.1.2. produzidos ou prestados por empresas brasileiras;

7.25.1.3. produzidos ou prestados por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

7.25.1.4. produzidos ou prestados por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação.

7.26. Persistindo o empate, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas empatadas.

7.27. Antes de seguir para a etapa de negociação, o pregoeiro irá certificar-se de que o licitante detentor da proposta vencedora enviou, por meio do sistema, os documentos de habilitação exigidos no edital e a proposta

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

de preços, nos termos do item 5 - DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO - deste Edital e, caso não tenha sido cumprida a exigência, a proposta será desclassificada.

7.28. Encerrada a etapa de envio de lances da sessão pública, o pregoeiro deverá encaminhar, pelo sistema eletrônico, contraproposta ao licitante que tenha apresentado o melhor preço, para que seja obtida melhor proposta, vedada a negociação em condições diferentes das previstas neste Edital.

7.28.1. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

7.29. Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

8. DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

8.1 O pregoeiro convocará o licitante melhor classificado para apresentar **no prazo de até 2 (duas) horas**, por meio do sistema eletrônico, **a proposta de preços final** ajustada à negociação realizada, acompanhada, se for o caso, de documentos complementares, quando necessários para confirmação de outro documento ou informação apresentados.

8.2. A proposta de preços final deverá:

8.2.1. ser redigida em língua portuguesa, datilografada ou digitada, em uma via, sem emendas, rasuras, entrelinhas ou ressalvas, devendo a última folha ser assinada e as demais rubricadas pelo licitante ou seu representante legal;

8.2.2. conter a identificação do licitante, os preços ofertados, em conformidade com último lance apresentado ou à negociação efetuada com o Pregoeiro, podendo utilizar como modelo o Anexo II deste Edital – Modelo de Proposta;

8.2.3. apresentar os preços ofertados, devidamente ajustados ao lance vencedor;

8.2.4. conter a indicação do banco, número da conta e agência do licitante vencedor, para fins de pagamento;

8.2.5. Somente mediante autorização do Pregoeiro e em caso de indisponibilidade do sistema, será aceito o envio da documentação por meio do e-mail licitacao@crcmg.org.br.

8.2.6. O prazo para envio da proposta poderá ser prorrogado, mediante solicitação escrita e justificada do licitante, via chat do sistema Comprasnet, formulada antes de findo o prazo estabelecido e formalmente aceita pelo Pregoeiro.

8.3. A proposta final deverá ser documentada nos autos e será levada em consideração no decorrer da execução do contrato e aplicação de eventual sanção à Contratada, se for o caso.

8.3.1. Todas as especificações do objeto contidas na proposta vinculam a Contratada.

8.4. Os preços deverão ser expressos em moeda corrente nacional, o valor unitário em algarismos e o valor global em algarismos e por extenso (art. 5º da Lei nº 8.666/93).

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

8.4.1. Ocorrendo divergência entre os preços unitários e o preço global, prevalecerão os primeiros; no caso de divergência entre os valores numéricos e os valores expressos por extenso, prevalecerão estes últimos.

8.5. A oferta deverá ser firme e precisa, limitada, rigorosamente, ao objeto deste Edital, sem conter alternativas de preço ou de qualquer outra condição que induza o julgamento a mais de um resultado, sob pena de desclassificação.

8.6. A proposta deverá obedecer aos termos deste Edital e seus Anexos, não sendo considerada aquela que não corresponda às especificações ali contidas ou que estabeleça vínculo à proposta de outro licitante.

8.7. As propostas que contenham a descrição do objeto, o valor e os documentos complementares estarão disponíveis na internet, após a homologação.

9. DA ACEITABILIDADE DA PROPOSTA VENCEDORA

9.1. Encerrada a etapa de negociação, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no parágrafo único do art. 7º e no § 9º do art. 26 do Decreto n.º 10.024/2019.

9.2. Será desclassificada a proposta ou o lance vencedor que apresentar preço final superior ao preço máximo fixado (Acórdão nº 1455/2018 - TCU - Plenário), ou que apresentar preço manifestamente inexequível.

9.2.1. Considera-se inexequível a proposta que apresente preços global ou unitários simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da licitação não tenha estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do próprio licitante, para os quais ele renuncie a parcela ou à totalidade da remuneração.

9.3. Qualquer interessado poderá requerer que se realizem diligências para aferir a exequibilidade e a legalidade das propostas, devendo apresentar as provas ou os indícios que fundamentam a suspeita;

9.3.1. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento das propostas, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, vinte e quatro horas de antecedência, e a ocorrência será registrada em ata;

9.4. O Pregoeiro poderá convocar o licitante para enviar documento digital complementar, por meio de funcionalidade disponível no sistema, **no prazo de 2 (duas) horas**, sob pena de não aceitação da proposta.

9.4.1. O prazo estabelecido poderá ser prorrogado pelo Pregoeiro por solicitação escrita e justificada do licitante, formulada antes de findo o prazo, e formalmente aceita pelo Pregoeiro.

9.4.2. Dentre os documentos passíveis de solicitação pelo Pregoeiro, destacam-se a Planilha de Custos e Formação de Preços, bem como os que contenham as características do material ofertado, tais como marca, modelo, tipo, fabricante e procedência, além de outras informações pertinentes, a exemplo de catálogos, folhetos ou propostas, encaminhados por meio eletrônico, ou, se for o caso, por outro meio e prazo indicados pelo Pregoeiro, sem prejuízo do seu ulterior envio pelo sistema eletrônico, sob pena de não aceitação da proposta.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

9.5. Será desclassificada a proposta ou o lance vencedor, nos termos do item 9.1 do Anexo VII-A da In SEGES/MP n. 5/2017, que:

9.5.1. não estiver em conformidade com os requisitos estabelecidos neste edital;

9.5.2. contenha vício insanável ou ilegalidade;

9.5.3. não apresente as especificações técnicas exigidas pelo Termo de Referência;

9.5.4. apresentar preço final superior ao preço máximo fixado (Acórdão nº 1455/2018 -TCU - Plenário), ou que apresentar preço manifestamente inexequível.

9.5.4.1. Quando o licitante não conseguir comprovar que possui ou possuirá recursos suficientes para executar a contento o objeto, será considerada inexequível a proposta de preços ou menor lance que:

9.5.4.1.1. for insuficiente para a cobertura dos custos da contratação, apresente preços global ou unitários simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da licitação não tenha estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do próprio licitante, para os quais ele renuncie a parcela ou à totalidade da remuneração.

9.5.4.1.2. apresentar um ou mais valores da planilha de custo que sejam inferiores àqueles fixados em instrumentos de caráter normativo obrigatório, tais como leis, medidas provisórias e convenções coletivas de trabalho vigentes.

9.6. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, na forma do § 3º do artigo 43 da Lei nº 8.666, de 1993 e a exemplo das enumeradas no item 9.4 do Anexo VII-A da IN SEGES/MP N. 5, de 2017, para que a empresa comprove a exequibilidade da proposta.

9.7. Quando o licitante apresentar preço final inferior a 30% (trinta por cento) da média dos preços ofertados para o mesmo item, e a inexequibilidade da proposta não for flagrante e evidente pela análise da planilha de custos, não sendo possível a sua imediata desclassificação, será obrigatória a realização de diligências para aferir a legalidade e exequibilidade da proposta.

9.8. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante do serviço ou da área especializada no objeto.

9.9. Se a proposta ou lance vencedor for desclassificado, o Pregoeiro examinará a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação.

9.10. Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a continuidade da mesma.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

9.11. Nos itens não exclusivos para a participação de microempresas e empresas de pequeno porte, sempre que a proposta não for aceita, e antes de o Pregoeiro passar à subsequente, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida, se for o caso.

9.12. Encerrada a análise quanto à aceitação da proposta, o pregoeiro verificará a habilitação do licitante, observado o disposto neste Edital

10. DA HABILITAÇÃO

10.1. Como condição prévia ao exame da documentação de habilitação do licitante detentor da proposta classificada em primeiro lugar, o Pregoeiro verificará o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

10.1.1. SICAF;

10.1.2. Consulta Consolidada de Pessoa Jurídica do Tribunal de Contas da União (<https://certidoes-apf.apps.tcu.gov.br/>);

10.1.3. Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS, mantido pela Controladoria-Geral da União (<https://portal.datransparencia.gov.br/sancoes/consulta?ordenarPor=nomeSancionado&direcao=asc>);

10.1.4. Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça. (www.cnj.jus.br/improbidade_adm/consultar_requerido.php);

10.1.5. Lista de Inidôneos, mantida pelo Tribunal de Contas da União – TCU (<https://contas.tcu.gov.br/ords/f?p=1660:3:0>).

10.1.6. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força do artigo 12 da Lei nº 8.429, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.

10.1.6.1. Caso conste na Consulta de Situação do Fornecedor a existência de Ocorrências Impeditivas Indiretas, o gestor diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

10.1.6.1.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.

10.1.6.1.2. O licitante será convocado para manifestação previamente à sua desclassificação.

10.1.7. Constatada a existência de sanção, o Pregoeiro reputará o licitante inabilitado, por falta de condição de participação.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

10.1.8. No caso de inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos arts. 44 e 45 da Lei Complementar nº 123/2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

10.2. Caso atendidas as condições de participação, a habilitação do licitante será verificada por meio do Sistema de Cadastro Unificado de Fornecedores – SICAF, nos documentos por ele abrangidos, em relação à habilitação jurídica, à regularidade fiscal, à qualificação econômica financeira e habilitação técnica, conforme o disposto na Instrução Normativa SEGES/MP nº 03, de 2018.

10.2.1. O interessado, para efeitos de habilitação prevista na Instrução Normativa SEGES/MP nº 03, de 2018 mediante utilização do sistema, deverá atender às condições exigidas no cadastramento no SICAF até o terceiro dia útil anterior à data prevista para recebimento das propostas.

10.2.2. É dever do licitante atualizar previamente as comprovações constantes do SICAF para que estejam vigentes na data da abertura da sessão pública, ou encaminhar, em conjunto com a apresentação da proposta, a respectiva documentação atualizada.

10.2.3. O descumprimento do subitem acima implicará a inabilitação do licitante, exceto se a consulta aos sítios eletrônicos oficiais emissores de certidões feita pelo Pregoeiro lograr êxito em encontrar a(s) certidão(ões) válida(s), conforme art. 43, §3º, do Decreto 10.024, de 2019.

10.3. Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Edital e já apresentados, o licitante será convocado a encaminhá-los, em formato digital, via sistema, **no prazo de 2 (duas) horas**, sob pena de inabilitação.

10.3.1. O prazo para envio da documentação, acima previsto, poderá ser prorrogado, mediante solicitação escrita e justificada do licitante, via chat do sistema Comprasnet, formulada antes de findo o prazo estabelecido e formalmente aceita pelo Pregoeiro.

10.3.2. Somente mediante autorização do Pregoeiro e em caso de indisponibilidade do sistema, será aceito o envio da documentação por meio do e-mail licitacao@crcmg.org.br.

10.4. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não digitais quando houver dúvida em relação à integridade do documento digital.

10.4.1. Na hipótese de serem solicitados pelo pregoeiro, os documentos serão remetidos em original, por qualquer processo de cópia reprográfica, autenticada por tabelião de notas, ou por servidor da Administração, desde que conferidos com o original, ou publicação em órgão da imprensa oficial, para análise, no prazo de 2 (dois) dias úteis, à Gerência Administrativa e Financeira, para o endereço, rua Cláudio Manoel, 639, bairro Savassi, Belo Horizonte-MG, CEP 30.140-105, em envelope fechado e rubricado no fecho, especificando o número do pregão e os dados da empresa.

10.5. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

10.6. Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se o licitante for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

10.6.1. Serão aceitos registros de CNPJ de licitante matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

10.7. Ressalvado o disposto no item 5.3, os licitantes deverão encaminhar, nos termos deste Edital, a documentação relacionada nos itens a seguir, para fins de habilitação.

10.8. Habilitação Jurídica

10.8.1. No caso de Microempreendedor Individual – MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio www.portaldoempreendedor.gov.br;

10.8.2. No caso de empresário individual, inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

10.8.3. No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;

10.8.4. Inscrição no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz, no caso de ser o participante sucursal, filial ou agência;

10.8.5. No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

10.8.6. Decreto de autorização, em se tratando de sociedade empresária estrangeira em funcionamento no País;

10.8.7. No caso de sociedade cooperativa: ata de fundação e estatuto social em vigor, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, bem como o registro de que trata o art. 107 da Lei nº 5.764, de 1971.

10.8.8. Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

10.9. Regularidade Fiscal e Trabalhista

10.9.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso.

10.9.2. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

10.9.3. Prova de regularidade perante o Fundo de Garantia por Tempo de Serviço – FGTS (Certificado de Regularidade do FGTS – CRF).

10.9.4. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de Certidão Negativa ou Positiva com Efeito de Negativa de Débitos Trabalhistas – CNDT, expedida pelo Tribunal Superior do Trabalho, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei 5.452, de 1º de maio de 1943.

10.9.5. Prova de inscrição no cadastro de contribuintes municipal, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

10.9.6. Prova de regularidade com a Fazenda Municipal do domicílio ou sede do licitante, relativa à atividade em cujo exercício contrata ou concorre;

10.9.7. Caso o licitante seja considerado isento dos tributos municipais relacionados ao objeto licitatório, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda Municipal do seu domicílio ou sede, ou outra equivalente, na forma da lei;
OU

10.9.5. Prova de inscrição no cadastro de contribuintes estadual, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

10.9.6. Prova de regularidade com a Fazenda Estadual do domicílio ou sede do licitante, relativa à atividade em cujo exercício contrata ou concorre;

10.9.7. Caso o licitante seja considerado isento dos tributos estaduais relacionados ao objeto licitatório, deverá comprovar tal condição mediante declaração da Fazenda Estadual do seu domicílio ou sede, ou outra equivalente, na forma da lei;

10.9.8. Caso o licitante detentor do menor preço seja qualificado como microempresa ou empresa de pequeno porte deverá apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição, sob pena de inabilitação.

10.10. Qualificação Econômico-Financeira

10.10.1. Certidão negativa de falência ou recuperação judicial, ou liquidação judicial, ou de execução patrimonial, conforme o caso, expedida pelo distribuidor da sede do licitante ou de seu domicílio, dentro do prazo de validade previsto na própria certidão, ou, na omissão desta, expedida há menos de 1 (um) ano contado da data da sua apresentação.

10.10.1.1. No caso de certidão positiva de recuperação judicial ou extrajudicial, o licitante deverá apresentar a comprovação de que o respectivo plano de recuperação foi acolhido judicialmente, na forma do art. 58, da Lei n.º 11.101, de 09 de fevereiro de 2005, sob pena de inabilitação, devendo, ainda, comprovar todos os demais requisitos de habilitação.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

10.10.1.2. Caso não conste no cadastro do SICAF do fornecedor a Certidão Negativa de Pedido de Falência e Concordata, o documento poderá ser consultado, pelo Pregoeiro, nos respectivos sítios oficiais emissores.

10.10.2. Balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta;

10.10.2.1. no caso de empresa constituída no exercício social vigente, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade;

10.10.2.2. é admissível o balanço intermediário, se decorrer de lei ou contrato/estatuto social.

10.10.3. comprovação da boa situação financeira da empresa mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), obtidos pela aplicação das seguintes fórmulas:

$$\begin{aligned}
 \text{LG} &= \frac{\text{Ativo Circulante} + \text{Realizável a Longo Prazo}}{\text{Passivo Circulante} + \text{Passivo Não Circulante}} \\
 \text{SG} &= \frac{\text{Ativo Total}}{\text{Passivo Circulante} + \text{Passivo Não Circulante}} \\
 \text{LC} &= \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}
 \end{aligned}$$

10.10.4. As empresas, cadastradas ou não no SICAF, que apresentarem resultado inferior ou igual a 1(um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverão comprovar patrimônio líquido de 10% (dez por cento) do valor estimado da contratação ou do item pertinente.

10.11. Qualificação técnica operacional e profissional

10.11.1. Qualificação técnica operacional

10.11.1.1. Como qualificação técnica, o licitante deverá apresentar juntamente com os documentos de habilitação, pelo menos 01 (um) atestado de capacidade técnica, expedido por pessoa jurídica de direito público ou privado, que comprove ter prestado serviços, pelo prazo mínimo de 12 (doze) meses, condizentes minimamente com os seguintes serviços solicitados neste termo de referência, sendo válida a apresentação de mais de um documento para a comprovação do quantitativo exigido, sendo os serviços de maior relevância:

10.11.1.1.1. Serviço de Gestão de Vulnerabilidades, por meio do fornecimento, instalação, prestação de serviços de suporte, administração e operação da solução para no mínimo, 150 (cento e cinquenta) ativos de TI. Este item visa atestar a capacidade da licitante para o fornecimento do serviço especificado no Item SERVIÇO DE GESTÃO VULNERABILIDADE exigido neste certame.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

10.11.1.1.2. Serviços Gerenciado de monitoramento, triagem, tratamento e resposta a incidentes de segurança, utilizando tecnologia de SIEM (Security Information and Event Management) para gerenciamento e correlação de eventos de segurança através da análise de Logs e pacotes, em redes com, no mínimo, 150 (centos e cinquenta) ativos de TI.

10.11.1.1.3. Disponibilidade de Centro de Operações de Segurança que disponha de dois tipos de conexões digitais com a CONTRATADA, a fim de garantir a redundância e disponibilidade das conexões do Centro de Operações de Segurança.

10.11.1.2. O atestado deverá ser apresentado em papel timbrado da pessoa jurídica, contendo a identificação do signatário, nome, endereço, telefone e, se for o caso, correio eletrônico, para contato, e deve indicar as características, quantidades e prazos das atividades executadas ou em execução pela licitante vencedora.

10.11.1.3. Os atestados de capacidade técnica apresentados poderão ser objeto de diligência a critério do CRCMG, para verificação da autenticidade de seu conteúdo. Encontrada qualquer divergência entre a informação apresentada pela licitante vencedora e o apurado em eventual diligência, inclusive validação do contrato de prestação de serviço assinado entre o emissor e a licitante, além da desclassificação sumária do Pleito, a empresa fica sujeita às penalidades cabíveis e aplicáveis.

10.11.1.4. Para a comprovação da experiência mínima de 12 (doze) meses, será aceito o somatório de atestados de períodos diferentes.

10.11.2. Qualificação técnica profissional

10.11.2.1. Declaração formal de disponibilidade técnica, em papel timbrado da licitante, atestando que terá disponível, em seu quadro de pessoal, quando da assinatura do contrato e o consequente início da prestação dos serviços, equipe de profissionais com as qualificações técnicas obrigatórias e necessárias à execução dos serviços, objeto deste Edital, devendo constar as informações como, cargo, certificações e descrições acerca dos conhecimentos e experiências, conforme modelo de declaração constante do Anexo VII - Declaração Formal de Disponibilidade Técnica - Qualificação Técnica dos Profissionais da Empresa.

10.11.2.1.1. As certificações e os conhecimentos e experiências dos profissionais deverão atender aos requisitos mínimos estabelecidos no Termo de Referência, conforme modelo de declaração constante do Anexo VII, para cada profissional, de acordo com sua área de atuação, sob pena de desclassificação da licitante.

10.11.2.1.2. No momento da assinatura do contrato, a empresa deverá comprovar o vínculo com os referidos profissionais, apresentando cópia da Carteira de Trabalho e Previdência Social (CTPS), no caso de haver relação de emprego, ou de contrato de prestação de serviços, regidos pela legislação civil.

10.11.2.1.3. Em todo caso, os profissionais deverão estar disponíveis à prestação dos serviços de modo permanente, durante toda a vigência contratual.

10.11.2.1.4. Não serão aceitos vínculos de natureza eventual ou precária, inclusive os decorrentes de terceirização ou subcontratação.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

10.11.3. Vistoria

10.11.3.1. **Atestado de vistoria** assinado pelo responsável técnico do CRCMG, conforme modelo constante do **Anexo V**, ou Declaração de ciência das informações e condições do local de execução dos serviços, conforme modelo constante do **Anexo VI**, assinada por representante da licitante, assumindo todos riscos e consequências relativos às condições dos locais de execução do objeto e peculiaridades inerentes à natureza do trabalho, podendo a licitante, escolher entre as duas opções, a que melhor estiver adequada para sua participação no certame.

10.11.3.2. Ressalta-se que **a vistoria não é obrigatória**. Contudo, caso o licitante não tenha interesse em realizá-la, deverá preencher e incluir no sistema eletrônico juntamente com os demais documentos de habilitação, a **Declaração de ciência das informações e condições do local de execução dos serviços**, conforme modelo constante do **Anexo VI**.

10.11.3.3. Caso o licitante opte por fazer a vistoria deverá agendá-la, com antecedência mínima de 3 (três) dias da data de abertura da sessão, através do e-mail licitacao@crcmg.org.br.

10.12. O licitante enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado (a) da prova de inscrição nos cadastros de contribuintes estadual e municipal e (b) da apresentação do balanço patrimonial e das demonstrações contábeis do último exercício.

10.13. A existência de restrição relativamente à regularidade fiscal e trabalhista não impede que a licitante qualificada como microempresa ou empresa de pequeno porte seja declarada vencedora, uma vez que atenda a todas as demais exigências do edital.

10.13.1. A declaração do vencedor acontecerá no momento imediatamente posterior à fase de habilitação.

10.14. Caso a proposta mais vantajosa seja ofertada por microempresa, empresa de pequeno porte ou sociedade cooperativa equiparada, e uma vez constatada a existência de alguma restrição no que tange à regularidade fiscal e trabalhista, a mesma será convocada para, no prazo de 5 (cinco) dias úteis, após a declaração do vencedor, comprovar a regularização. O prazo poderá ser prorrogado por igual período, a critério da administração pública, quando requerida pelo licitante, mediante apresentação de justificativa.

10.15. A não regularização fiscal e trabalhista no prazo previsto no subitem anterior acarretará a inabilitação do licitante, sem prejuízo das sanções previstas neste Edital, sendo facultada a convocação dos licitantes remanescentes, na ordem de classificação. Se, na ordem de classificação, seguir-se outra microempresa, empresa de pequeno porte ou sociedade cooperativa com alguma restrição na documentação fiscal e trabalhista, será concedido o mesmo prazo para regularização.

10.16. Havendo necessidade de analisar minuciosamente os documentos exigidos, o Pregoeiro suspenderá a sessão, informando no "chat" a nova data e horário para a continuidade da mesma.

10.17. Será inabilitado o licitante que não comprovar sua habilitação, seja por não apresentar quaisquer dos documentos exigidos, ou apresentá-los em desacordo com o estabelecido neste Edital.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

10.18. Nos itens não exclusivos a microempresas e empresas de pequeno porte, em havendo inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

10.18.1. O licitante provisoriamente vencedor em um item, que estiver concorrendo em outro item, ficará obrigado a comprovar os requisitos de habilitação cumulativamente, isto é, somando as exigências do item em que venceu às do item em que estiver concorrendo, e assim sucessivamente, sob pena de inabilitação, além da aplicação das sanções cabíveis.

10.18.1.1. Não havendo a comprovação cumulativa dos requisitos de habilitação, a inabilitação recairá sobre o(s) item(ns) de menor(es) valor(es), cuja retirada(s) seja(m) suficiente(s) para a habilitação do licitante nos remanescentes.

10.19. Constatado o atendimento às exigências de habilitação fixadas no Edital, o licitante será declarado vencedor.

11. DOS RECURSOS

11.1. O Pregoeiro declarará o vencedor e, depois de decorrida a fase de regularização fiscal e trabalhista de microempresa ou empresa de pequeno porte, se for o caso, concederá o prazo de, no mínimo, trinta minutos, para que qualquer licitante manifeste a intenção de recorrer, de forma motivada, isto é, indicando contra qual(is) decisão(ões) pretende recorrer e por quais motivos, em campo próprio do sistema.

11.2. Havendo quem se manifeste, caberá ao Pregoeiro verificar a tempestividade e a existência de motivação da intenção de recorrer, para decidir se admite ou não o recurso, fundamentadamente.

11.2.1. Nesse momento o Pregoeiro não adentrará no mérito recursal, mas apenas verificará as condições de admissibilidade do recurso.

11.2.2. A falta de manifestação motivada do licitante quanto à intenção de recorrer importará a decadência desse direito.

11.2.3. Uma vez admitido o recurso, o recorrente terá, a partir de então, o prazo de três dias para apresentar as razões, pelo sistema eletrônico, ficando os demais licitantes, desde logo, intimados para, querendo, apresentarem contrarrazões também pelo sistema eletrônico, em outros três dias, que começarão a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa de seus interesses.

11.2.4. Caso o licitante que manifestou intenção de recorrer não apresente o recurso fundamentado no sistema eletrônico dentro do prazo acima estabelecido, decaíra seu direito recursal e o pregoeiro dará prosseguimento à fase de adjudicação.

11.2.5. A Administração decidirá sob o recurso e enviará resposta no sistema eletrônico no prazo máximo de 10 (dez) dias contados do encerramento do prazo de contrarrazões.

11.3. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

11.4. Os autos do processo permanecerão com vista franqueada aos interessados, no endereço constante neste Edital.

12. DA REABERTURA DA SESSÃO PÚBLICA

12.1. A sessão pública poderá ser reaberta:

12.1.1. Nas hipóteses de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que dele dependam.

12.1.2. Quando houver erro na aceitação do preço melhor classificado ou quando o licitante declarado vencedor não assinar o contrato, não retirar o instrumento equivalente ou não comprovar a regularização fiscal, nos termos do art. 43, §1º da LC nº 123/2006. Nessas hipóteses, serão adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.

12.2. Todos os licitantes remanescentes deverão ser convocados para acompanhar a sessão reaberta.

12.2.1. A convocação se dará por meio do sistema eletrônico ("chat") ou e-mail, de acordo com a fase do procedimento licitatório.

12.2.2. A convocação feita por e-mail dar-se-á de acordo com os dados contidos no SICAF, sendo responsabilidade do licitante manter seus dados cadastrais atualizados.

13. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

13.1. O objeto da licitação será adjudicado à licitante declarada vencedora, por ato do Pregoeiro, caso não haja interposição de recurso, ou pela autoridade competente, após a regular decisão dos recursos apresentados.

13.2. Após a fase recursal, constatada a regularidade dos atos praticados, a autoridade competente homologará o procedimento licitatório.

14. DA GARANTIA DE EXECUÇÃO

14.1. Será exigida a prestação de garantia de execução, na presente contratação, conforme regras constantes do Contrato.

15. DO TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE

15.1. Após a homologação da licitação, em sendo realizada a contratação, será firmado Termo de Contrato ou emitido instrumento equivalente.

15.2. O adjudicatário terá o prazo de 5 (cinco) dias úteis, contados a partir da data de sua convocação, para assinar o Termo de Contrato ou aceitar instrumento equivalente, conforme o caso (Nota de Empenho/Carta Contrato/Autorização), sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

15.2.1. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do Termo de Contrato ou aceite do instrumento equivalente, a Administração poderá encaminhá-lo para assinatura ou aceite

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

da Adjudicatária, mediante correspondência postal com aviso de recebimento (AR) ou meio eletrônico, para que seja assinado e devolvido ou aceito no prazo de 5 (cinco) dias úteis, a contar da data de seu recebimento.

15.2.2. O prazo previsto no subitem anterior poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

15.3. O Aceite da Nota de Empenho ou do instrumento equivalente, emitida à empresa adjudicada, implica no reconhecimento de que:

15.3.1. referida Nota está substituindo o contrato, aplicando-se à relação de negócios ali estabelecida as disposições da Lei nº 8.666, de 1993;

15.3.2. a contratada se vincula à sua proposta e às previsões contidas no edital e seus anexos;

15.3.3. a contratada reconhece que as hipóteses de rescisão são aquelas previstas nos artigos 77 e 78 da Lei nº 8.666/93 e reconhece os direitos da Administração previstos nos artigos 79 e 80 da mesma Lei.

15.4. Previamente à contratação a Administração realizará consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018, e nos termos do art. 6º, III, da Lei nº 10.522, de 19 de julho de 2002, consulta prévia ao CADIN.

15.4.1. Nos casos em que houver necessidade de assinatura do instrumento de contrato, e o fornecedor não estiver inscrito no SICAF, este deverá proceder ao seu cadastramento, sem ônus, antes da contratação.

15.4.2. Na hipótese de irregularidade do registro no SICAF, o contratado deverá regularizar a sua situação perante o cadastro no prazo de até 05 (cinco) dias úteis, sob pena de aplicação das penalidades previstas no edital e anexos.

15.5. Na assinatura do contrato ou da ata de registro de preços, será exigida a comprovação das condições de habilitação consignadas no edital, que deverão ser mantidas pelo licitante durante a vigência do contrato ou da ata de registro de preços.

15.6. Na hipótese de o vencedor da licitação não comprovar as condições de habilitação consignadas no edital ou se recusar a assinar o contrato ou a ata de registro de preços, a Administração, sem prejuízo da aplicação das sanções das demais cominações legais cabíveis a esse licitante, poderá convocar outro licitante, respeitada a ordem de classificação, para, após a comprovação dos requisitos para habilitação, analisada a proposta e eventuais documentos complementares e, feita a negociação, assinar o contrato ou a ata de registro de preços.

15.7. As condições de entrega, de pagamento, vigência, reajuste, recebimento do objeto e fiscalização, obrigações da contratada e do contratante, sanções e rescisão obedecerão às disposições constantes do Termo de Referência – Anexo I deste Edital e da Lei nº 8.666/93.

16. DAS SANÇÕES ADMINISTRATIVAS.

16.1. Comete infração administrativa, nos termos da Lei nº 10.520/2002, o licitante/adjudicatária que:

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

16.1.1. Não assinar o termo de contrato ou aceitar/retirar o instrumento equivalente, quando convocada dentro do prazo de validade da proposta, salvo caso fortuito ou força maior;

16.1.2. Deixar de entregar a documentação exigida para o certame;

16.1.3. Apresentar documentação falsa exigida para o certame;

16.1.4. Não manter a proposta;

16.1.5. Cometer fraude fiscal; e

16.1.6. Comportar-se de modo inidôneo.

16.2. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

16.3. O licitante/adjudicatário que cometer qualquer das infrações discriminadas nos subitens anteriores, ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

16.3.1. Advertência por faltas leves, assim entendidas como aquelas que não acarretarem prejuízos significativos ao objeto da contratação

16.3.2. Multa de 10% (dez por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do licitante;

16.3.3. Suspensão temporária do direito de participar de licitação e impedimento de contratar com a Administração, pelo prazo de até 2 (dois) anos;

16.3.4. Impedimento de licitar e de contratar com órgãos e entidades da União e descredenciamento no SICAF, pelo prazo de até 5 (cinco) anos.

16.3.5. Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados;

16.4. A penalidade de multa pode ser aplicada cumulativamente com as demais sanções.

16.5. Se, durante o processo de aplicação de penalidade, houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

16.6. A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

16.7. Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

16.8. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente na Lei nº 9.784, de 1999.

16.9. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

16.10. As penalidades serão obrigatoriamente registradas no SICAF.

16.11. As sanções por atos praticados no decorrer da contratação estão previstas no Termo de Referência – Anexo I deste Edital.

17. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

17.1. Até 3 (três) dias úteis antes da data fixada para abertura da sessão pública, qualquer pessoa poderá impugnar este Edital.

17.2. A impugnação poderá ser realizada de forma eletrônica, pelo e-mail licitacao@crcmg.org.br ou por petição dirigida ou protocolada no endereço da sede do CRCMG, Rua Cláudio Manoel, 639, Savassi, Belo Horizonte – MG.

17.3. Caberá ao Pregoeiro, auxiliado pelos responsáveis pela elaboração deste Edital e seus anexos, decidir sobre a impugnação no prazo de até 2 (dois) dias úteis contados da data de recebimento da impugnação.

17.4. Acolhida a impugnação, será designada nova data para a realização do certame, exceto quando, inquestionavelmente, a alteração não afetar a formulação das propostas.

17.5. Os pedidos de esclarecimentos referentes a este processo licitatório deverão ser enviados ao Pregoeiro, até 3 (três) dias úteis anteriores à data fixada para abertura da sessão pública, por meio eletrônico, através do endereço www.comprasgovernamentais.gov.br ou pelo e-mail licitacao@crcmg.org.br.

17.6. O Pregoeiro responderá aos pedidos de esclarecimentos no prazo de 2 (dois) dias úteis, contado da data de recebimento do pedido, e poderá requisitar subsídios formais aos responsáveis pela elaboração do Edital e dos anexos.

17.7. As respostas aos pedidos de esclarecimentos serão divulgadas pelo sistema e vincularão os participantes e a Administração.

17.8. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

17.8.1. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo pregoeiro, nos autos do processo de licitação.

17.9. As respostas às impugnações e aos pedidos de esclarecimentos também serão disponibilizadas no sítio do CRCMG www.crcmg.org.br.

18. DAS DISPOSIÇÕES GERAIS

18.1. Da sessão pública do Pregão divulgar-se-á Ata no sistema eletrônico.

18.2. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo Pregoeiro.

18.3. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília – DF.

18.4. O licitante será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas e lances.

18.5. Incumbirá à licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

18.6. No julgamento das propostas e da habilitação, o Pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

18.7. A homologação do resultado desta licitação não implicará direito à contratação.

18.8. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

18.9. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

18.10. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.

18.11. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

18.12. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

18.13. O Edital está disponibilizado, na íntegra, no endereço eletrônico www.crcmg.org.br, e também poderão ser lidos e/ou obtidos na sede do CRCMG no endereço Rua Cláudio Manoel, nº 639, Savassi, Belo Horizonte - MG, nos dias úteis, no horário das 9h às 17h, mesmo endereço e período no qual os autos do processo administrativo permanecerão com vista franqueada aos interessados.

18.14. O licitante é responsável pela fidelidade e legitimidade das informações prestadas e dos documentos apresentados em qualquer fase da licitação. A falsidade de qualquer documento apresentado ou a inverdade das informações nele contidas implicará a imediata desclassificação do licitante que o tiver apresentado, ou, caso tenha sido o vencedor, a rescisão do contrato, sem prejuízo das demais sanções cabíveis.

18.15. A comunicação entre o Pregoeiro e os licitantes será realizada, exclusivamente, por meio das ferramentas disponíveis no sistema Comprasnet, sendo vedado qualquer atendimento presencial ou por meio de ligações telefônicas.

18.16. É facultada ao Pregoeiro ou à autoridade superior do CRCMG, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou complementar a instrução do processo licitatório, vedada a inclusão posterior de documento ou informação que deveria constar no ato da sessão pública.

18.17. Após a abertura da sessão pública do pregão, não caberá desistência de proposta, salvo se por motivo justo decorrente de fato superveniente e aceito pelo Pregoeiro.

18.18. A presente licitação poderá ser anulada em qualquer tempo, desde que seja constatada irregularidade no processo e/ou em seu julgamento, ou revogada por conveniência do CRCMG, sem que caiba às licitantes qualquer indenização.

18.19. Os casos omissos serão resolvidos pelo Pregoeiro, nos termos da legislação pertinente e dos Princípios Gerais de Direito.

18.20. As dúvidas e divergências que, eventualmente, possam surgir e que não possam ser dirimidas diretamente entre as partes, ficarão sujeitas ao foro da Justiça Federal, Subseção de Belo Horizonte, renunciando-se a qualquer outro, por mais privilegiado que seja.

18.21. É de responsabilidade do licitante o acompanhamento do processo no sítio www.comprasgovernamentais.gov.br, até a data da realização da sessão pública, tendo em vista que quaisquer alterações referentes a este Edital serão disponibilizadas no referido endereço, opções Acesso Livre – Pregões – Agendados.

18.22. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

- 18.22.1. Anexo I - Termo de Referência;
- 18.22.2. Anexo II - Modelo de Proposta;
- 18.22.3. Anexo III - Minuta do Contrato;
- 18.22.4. Anexo IV - Catálogo de Serviço;
- 18.22.4. Anexo V - Atestado de Vistoria;
- 18.22.5. Anexo VI - Declaração de Ciência das Informações e Condições de Execução dos Serviços;



Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

18.22.6. Anexo VII - Declaração formal de disponibilidade técnica - Qualificação técnica dos profissionais da empresa;

18.22.7. Anexo VIII - Modelo de Termo de Confidencialidade e Sigilo do Prestador.

Belo Horizonte, 24 de janeiro de 2023.

Assinado digitalmente por:
SUELY MARIA MARQUES DE OLIVEIRA
CPF: 686.588.426-49
Certificado emitido por AC SOLUTI Multipla v5
Data: 23/01/2023 16:53:03 -03:00



Suely Maria Marques de Oliveira
Presidente do CRCMG

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

ANEXO I - TERMO DE REFERÊNCIA

1. DO OBJETO

Contratação de empresa especializada em SERVIÇOS GERENCIADOS DE SEGURANÇA.

2. INDICAÇÃO DE RECURSOS ORÇAMENTÁRIOS

Centro de Custo: 327

Projeto: 5002

Conta contábil: 6.3.1.3.02.01.005

3. JUSTIFICATIVA DO INTERESSE PÚBLICO EVIDENCIADO

Considerando que nos últimos anos temos visto diversas instituições públicas e privadas sofrendo constantes ataques cibernéticos, e tendo em vista a implantação da LGPD no CRCMG, que exige a adoção de medidas de segurança mais eficazes, torna-se indispensável a aplicação de boas práticas de segurança da informação no ambiente tecnológico do CRCMG, a fim de torna-lo mais seguro e menos suscetível a esses ataques.

Diante do crescimento exponencial de ameaças e ataques sofridos a empresas privadas e órgãos públicos no Brasil e no mundo, investimentos contínuos em segurança da informação são fundamentais para a mitigação de riscos de segurança associados ao negócio de maneira a resguardar a confidencialidade, a disponibilidade e a integridade das informações.

O cenário de ameaças à segurança da informação não se resume somente em ataques aos serviços de TI pela Internet. Tentativas de acesso não autorizado, infecção por arquivos maliciosos (vírus), e-mails indesejados (SPAMs), engenharia social, entre outros, são exemplos de eventos que podem apresentar riscos à segurança de TI. Até mesmo colaboradores não conscientes ou mal-intencionados representam risco potencial à segurança da informação.

Na busca de aperfeiçoamento da sua missão institucional e gestão pública, o Conselho Regional de Contabilidade de Minas Gerais vem utilizando cada vez mais soluções de TI, disponibilizando aos seus colaboradores, profissionais contábeis e à sociedade diversos serviços relacionados à Tecnologia da Informação. Nesse cenário, diversas foram as mudanças: tanto em termos de quantidade de serviços oferecidos quanto em diversidade de soluções, o que contribui para o aumento dos riscos e da necessidade de monitoramento, à medida que cresce a oferta de serviços pela Internet.

Nesse sentido, incidentes de segurança da informação, como nas hipóteses de violação, roubo ou perda de informações custodiadas pelo CRCMG, podem constituir possíveis situações capazes de inviabilizar, senão a totalidade, parte das atividades desta Entidade. Assim, a ocorrência de eventuais sinistros poderia provocar o vazamento de informações e prejuízo à sua imagem, podendo ainda o Conselho ter que responder pelos danos causados.

Por esses motivos, e devido ao incidente ocorrido recentemente no ambiente, tendo em vista que o Conselho não dispõe de infraestrutura física e pessoal para o monitoramento e gerenciamento de dispositivos de segurança com diversos fornecedores (firewall, sistema de prevenção de intrusões de rede, gerenciamento unificado de ameaças), capazes de realizar ações contra incidentes de segurança de forma tempestiva e procedimental, torna-se necessária realizar a contratação de uma solução que forneça uma estrutura em segurança da informação adequada, de forma a propiciar a integridade, confidencialidade, autenticidade e a

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

disponibilidade dos dados, através de um monitoramento preventivo e contínuo de segurança da informação contra ataques cibernéticos e de serviço de resposta a incidentes de segurança.

A contratação pretendida está alinhada com o planejamento estratégico do CRCMG, uma vez que contribuirá para o alcance do objetivo da qualidade de “Assegurar meios e recursos que permitam o cumprimento das políticas e diretrizes da gestão”, bem como dos objetivos estratégicos de “garantir qualidade e confiabilidade nos processos e nos procedimentos” e “Assegurar adequada infraestrutura e suporte logístico às necessidades dos CRCs”.

4. AMBIENTE TECNOLÓGICO DA CONTRATANTE (HARDWARE E SOFTWARE)

Infraestrutura tecnológica:

- 1 Firewall + 1 centralizador de logs, registros e relatórios como serviço;
- 129 estações de trabalho;
- 7 servidores virtuais Windows;
- 4 servidores virtuais Linux
- 90 usuários de rede;
- 125 caixas de e-mail na GSuite;

5. ESCOPO DOS SERVIÇOS

5.1. Serviços de monitoramento de ataques cibernéticos e resposta a incidentes:

- 5.1.1. Visa o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados à CONTRATANTE, através de fornecimento de solução de correlacionamento de logs de aplicações, serviços e infraestrutura do CONTRATANTE, que possam gerar eventos de segurança da informação, aos quais devem ser analisados, remediados, contidos e documentados, podendo estes serem transformados em um incidente de segurança da informação, obedecendo um processo cíclico e rigoroso de gestão de eventos.

5.2. Serviços de Gestão de Vulnerabilidades:

- 5.2.1. Tem por objetivo, de forma proativa e recorrente, identificar possíveis vulnerabilidades de segurança da informação na infraestrutura, nas aplicações e nas contas de usuários do CONTRATANTE, a fim de evitar que ataques cibernéticos direcionados à CONTRATANTE obtenha sucesso, explorando tais vulnerabilidades já conhecidas.

5.3. Serviço de monitoramento, detecção e resposta a incidentes para Endpoints.

- 5.3.1. Visa a proteção, monitoramento contínuo e operação de solução dedicada a proteção de estações e servidores do CONTRATANTE, realizando de forma proativa o bloqueio de códigos maliciosos tipo vírus, Malware - blindando os ativos protegidos também contra Ransomware, oferecendo possibilidade de realização de “Rollback” de arquivos alvos de códigos maliciosos, oferecendo ainda suporte à investigação de ataques através da trilha de registros de eventos forense.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

6. REQUISITOS GERAIS DOS SERVIÇOS

6.1. Os requisitos gerais dos serviços definem os requisitos obrigatórios para todos os serviços que compõem o objeto SERVIÇOS GERENCIADOS DE SEGURANÇA.

6.1.1. A CONTRATADA deverá cumprir com os prazos de detalhamento e as informações com a periodicidade referenciada neste documento, segmentados pelas modalidades de prestação de serviço.

6.1.2. Todos os entregáveis mensais referenciados neste documento, a partir do terceiro mês de contrato, deverão ser exibidos comparando com os dois meses anteriores para comparação gráfica de evolução e desempenho.

6.2. São apresentadas, a seguir, as especificações técnicas mínimas dos serviços a serem ofertados referentes ao objeto. Os termos “possui”, “permite”, “suporta” e “é” implicam no fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo “ou” implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo “e” implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções.

6.3. A CONTRATADA deverá possuir ao menos 01 (um) Centro de operação de segurança, atendendo, no mínimo, as seguintes características:

6.4. CANAIS DE COMUNICAÇÃO

6.4.1. Para abertura de solicitações, a CONTRATADA deverá disponibilizar 03 (três) tipos de canais de comunicação, a saber:

Grupo de Tecnologia	Classificação
Linha telefônica	Tipo 1
E-mail com domínio registrado e de propriedade da CONTRATADA.	Tipo 2
Sistema de ITSM do inglês <i>Information Technology Service Management</i> (Gerenciamento de Serviços de TI).	Tipo 3

Tabela 1- Tipos de canais de comunicação

6.4.2. Independente do canal de comunicação utilizado pela CONTRATANTE, as solicitações devem ser convergidas, atualizadas, resolvidas e concentradas em um único sistema de ITSM (Gerenciamento de Serviços de TI). Ou seja, imaginando que a CONTRATANTE realize a abertura de uma nova solicitação de serviço via linha telefônica, no segundo que segue a sua solicitação, a mesma deve constar no sistema de ITSM, assim também deve se proceder com a utilização do canal de comunicação do tipo 2: via e-mail.

6.4.3. Sobre o canal de comunicação do tipo 1: via linha telefonia tais ligações obrigatoriamente devem ser atendidas e/ou recepcionadas por uma interface humana, não sendo permitida a utilização de URA (Unidade de Resposta Audível), e/ou qualquer uso de atendimento eletrônico.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 6.4.4. Para um eventual cenário de crise, ou seja, onde o negócio fim da CONTRATANTE estiver sendo fortemente afetado por um problema envolvendo a segurança da informação, a CONTRATADA deverá disponibilizar uma sala de videoconferência virtual de sua propriedade, onde a qualquer tempo poderá ser utilizada para reuniões emergenciais para tratamento de crises.
- 6.4.5. Tal sala deve estar disponível via internet e seu acesso deve obrigatoriamente ser criptografado, utilizando protocolo SSL do inglês Secure Socket Layer, com certificado digital emitido em nome da CONTRATADA. A CONTRATADA também deve garantir que os canais de comunicação utilizados pela sala de videoconferência utilizem protocolos para criptografia dos dados trafegados.
- 6.4.6. A sala virtual ainda deve ter capacidade para minimamente 10 (dez) pessoas da CONTRATANTE simultaneamente, e a fim de evitar eventuais perdas de tempo em momento de crise, a sala deve estar acessível a qualquer tempo, não sendo criada apenas no momento da crise.

6.5. HORÁRIO DE ATENDIMENTO

- 6.5.1. Os SERVIÇOS GERENCIADOS DE SEGURANÇA devem obrigatoriamente ser executados, ofertados e estar acessíveis à CONTRATANTE em regime de 24 (vinte quatro) horas por dia, 07 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, durante todo o período de vigência do contrato.
- 6.5.2. Todo o atendimento deve ser iniciado por profissionais da contratada que estejam em horário de trabalho no momento do atendimento. Não é permitido o uso de funcionários no chamado "Regime de Plantão", "Sobreaviso" e/ou sistemas similares onde o funcionário apenas passa a trabalhar no momento do incidente.
- 6.5.3. GESTÃO DE CATÁLOGO DE SERVIÇO DO AMBIENTE DE SEGURANÇA DA INFORMAÇÃO**
- 6.5.3.1. A fim de fornecer uma única fonte de informação sobre os SERVIÇOS GERENCIADOS DE SEGURANÇA, disponíveis para cada grupo de tecnologia dos itens de configuração do parque de segurança da informação da CONTRATANTE, será definido em conjunto com a CONTRATADA uma lista de serviços que a CONTRATADA deverá ser capaz de entregar. Tal definição deverá ser aceita por ambas as partes e ficar disponível para consulta.
- 6.5.3.2. É de responsabilidade da CONTRATADA manter, atualizar e revisar os serviços disponíveis para cada grupo de serviço. As responsabilidades da CONTRATANTE estão relacionadas a aprovação de um novo serviço, ou a aposentadoria de um ou mais serviços existentes.
- 6.5.3.3. O catálogo de serviço deverá ser mantido e administrado através do sistema de ITSM de responsabilidade da CONTRATADA, estando este disponível de forma online para a CONTRATANTE, onde essa poderá consultar, a qualquer tempo, os serviços disponíveis.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

6.5.3.4. Apesar de já existir uma definição prévia de parte dos serviços a serem entregues pela CONTRATADA, incluídas no presente termo de referência (**Anexo VII - CATÁLOGO DE SERVIÇO**), a CONTRATANTE, a qualquer tempo, poderá solicitar a inclusão de novos serviços, ou a retirada de um serviço, em comum acordo com a CONTRATADA.

6.5.3.5. Também se espera que tais revisões de continuidade de um serviço no catálogo de serviços seja sugerido por parte da CONTRATADA durante a execução do contrato. Todavia, não é de responsabilidade da CONTRATADA a retirada ou inclusão de um serviço, cabendo apenas à CONTRATANTE tal ação.

6.5.4. MODALIDADE DE ATENDIMENTO

6.5.4.1. A modalidade preferencial de atendimento será a do tipo remota, devendo ser realizada nas dependências da CONTRATADA caso necessário, obedecendo, obrigatoriamente, os critérios estabelecidos para sua execução, conforme previstos neste Termo de Referência.

6.5.4.2. Os atendimentos referentes ao objeto contratado, denominado SERVIÇOS GERENCIADOS DE SEGURANÇA, são ilimitados durante o período de vigência do contrato, ou seja, não existe limite para quantidade de horas, e/ou quantidade de atendimentos realizados, limitando-se apenas ao escopo.

6.5.5. ACESSIBILIDADE E CONFIDENCIALIDADE

6.5.5.1. Para garantir a qualidade e disponibilidade dos serviços remotos, entre a CONTRATANTE e o Centro de Operações de Segurança da CONTRATADA, deverá haver dois tipos de conexões digitais, a fim de garantir a redundância e disponibilidade das conexões do Centro de Operações de Segurança.

6.5.5.2. Ambas as conexões digitais devem ter velocidade de upload e download mínima de 10 (dez) Mbps, serem contratadas de operadoras e rotas distintas, e devem ser utilizadas única e exclusivamente para prestação dos serviços presentes no Termo de Referência.

6.5.5.3. Especificamente para o tipo de conexão digital internet, necessariamente precisará ter IP dedicado, e não serão aceitos contratos com linksxDSL (executada a tecnologia HDSL). Também, a fim de garantir a disponibilidade da conexão, deverá a CONTRATADA garantir que tal conexão esteja protegida contra-ataques de DDoS - do inglês Distributed Denial of Service.

6.5.5.4. É de responsabilidade da CONTRATADA a contratação e os custos relativos ao fornecimento dos links de internet junto às operadoras, durante todo o período de vigência do contrato.

6.5.5.5. A fim de garantir a segurança do tráfego bidirecional entre a CONTRATANTE e o Centro de Operações de Segurança da CONTRATADA, ambas as conexões devem ser criptografadas. Ou seja, a CONTRATADA deverá estabelecer duas VPN's - do Inglês Virtual Private

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

Network, do tipo Site To Site, para o Centro de Operações de Segurança.

6.5.5.6. A fim de garantir a segurança entre a CONTRATANTE e os Centro de Operações de Segurança da CONTRATADA, não será permitido Centro de Operações de Segurança terceirizado ou consórcio de CONTRATANTES. A CONTRATADA deve ter e manter Centro de Operações de Segurança próprio.

6.5.5.7. Por outro lado, a CONTRATADA deve revogar todas as credenciais relacionadas a soluções de sua responsabilidade, empregadas na prestação de serviços para a CONTRATANTE, bem como solicitar tais revogações à CONTRATANTE, para soluções de responsabilidade da CONTRATADA, no mesmo dia do encerramento das atividades.

6.5.5.8. Tais exigências visam proteger o CONTRATANTE contra o uso indevido de informações sob sua custódia, por parte de profissional da CONTRATADA, assim como estão em conformidade com boas práticas de gestão e governança de TI.

6.5.6. DO CENTRO DE OPERAÇÕES DE CIBERSEGURANÇA - CSOC (CYBER SECURITY OPERATION CENTER)

6.5.6.1. Os SERVIÇOS GERENCIADOS DE SEGURANÇA devem ser executados por meio de ao menos 01 (um) Centro de Operações de Segurança da CONTRATADA, devendo estar situado obrigatoriamente no Brasil.

6.6. O CSOC deve atender os requisitos mínimos, a saber:

- 6.6.1. Utilizar sistema de gerenciamento de CFTV, que viabilizem o rastreamento de pessoas dentro do ambiente da CONTRATADA e cujas imagens possam ser recuperadas;
- 6.6.2. Filmar toda a área, mantendo as imagens armazenadas por, no mínimo, 90 (noventa) dias;
- 6.6.3. Efetuar registro de entrada e saída dos visitantes, com identificação individual em todos os acessos ao CSOC;
- 6.6.4. Possuir solução de monitoramento de disponibilidade e desempenho.
- 6.6.5. O perímetro físico do CSOC deve ser equipado com sensor de intrusão e alarmes contra acesso indevido;
- 6.6.6. Ser vigiado de forma ininterrupta em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano;
- 6.6.7. Ter controle de acesso físico com pelo menos 2 (dois) dos seguintes fatores de autenticação, a saber: cartão de identificação magnético, biometria de leitura de digital, reconhecimento facial e análise de retina;
- 6.6.8. Funcionar em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

(trezentos e sessenta e cinco) dias por ano;

- 6.6.9. Possuir registro de entrada e saída de pessoas, mantido por, pelo menos, 90 dias.
- 6.6.10. Possuir sistemas redundantes de alimentação de energia.
- 6.6.11. Para o caso de CSOC que utilize datacenter próprio, possuir estrutura de armazenamento de dados que permita a manutenção dos registros dos eventos relacionados aos serviços contratados por, no mínimo, o prazo do contrato.
- 6.6.12. Ser configurado de forma que a falha de um dos equipamentos isoladamente NÃO interrompa a prestação dos serviços;
- 6.6.13. Ter sistema de provimento ininterrupto de energia elétrica, composto por grupo gerador e UPSs do inglês Uninterruptible Power Supply, para garantir a transição entre o fornecimento normal da energia e o grupo gerador;
- 6.6.14. Para o caso de CSOC que utilize datacenter próprio, ter componentes de segurança necessários para garantir a preservação dos dados em casos de incêndio e execução de plano de recuperação de catástrofes;
- 6.6.15. Deverá possuir processos implementados baseados na norma ABNT NBR ISO/IEC 27001.
- 6.7. Para o caso de CSOC que utilize datacenter próprio, as infraestruturas de datacenter devem estar situadas fora dos ambientes de CSOC, e devem obrigatoriamente atender aos requisitos técnicos elencados, a saber:**
- 6.7.1. Estrutura física dedicada e construída com a finalidade exclusiva de prestação de serviços de hospedagem de aplicações e equipamentos, de modo a garantir um ambiente seguro e controlado, ou seja, não poderá possuir instalações hidráulicas na infraestrutura do Data Center;
- 6.7.2. Todos os equipamentos envolvidos na solução a ser disponibilizada deverão possuir fontes redundantes;
- 6.7.3. Deverá possuir área de estacionamento livre e privado, com acesso seguro para desembarque e manuseio de equipamentos com vigilância armada;
- 6.7.4. Deverá possuir guarita com segurança armada em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano. A guarita de segurança deverá estar fora do prédio de Data Center, criando-se uma barreira física ao acesso do Data Center, ter acesso a todo o sistema de CFTV, inclusive em tempo real, e detecção de intrusos em todas as cercanias onde está localizado o Data Center;
- 6.7.5. Toda a área do Data Center deve ser desprovida de janelas, básculas ou quaisquer formas de acesso que não através dos controles de acesso;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 6.7.6. Garantir a disponibilidade de pessoas dedicadas, treinadas e responsáveis pela segurança de acesso ao prédio e aos equipamentos do ambiente em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano;
- 6.7.7. Utilizar câmeras digitais de circuito interno de televisão, monitoradas e gerenciadas cujas imagens possam ser posteriormente consultadas por um período mínimo de 90 (noventa) dias, viabilizando o rastreamento de pessoas dentro do ambiente;
- 6.7.8. As câmeras digitais de circuito interno de televisão deverão cobrir todos os ângulos do túnel frio de forma que não existam quaisquer pontos cegos. A gravação e visualização em tempo real deverá ser feita em alta-resolução e em cores, com no mínimo 10 frames por segundo. Tais características são necessárias para que seja possível identificação da face daqueles que pretendem adentrar as cercanias do prédio do Data Center;
- 6.7.9. Sistema de detecção e combate a incêndio com uso de sensores de fumaça e fogo distribuídos pela área do Data Center e uso de descarga de gás com efeito supressor de combustão ou redução de oxigênio, ecologicamente aceitável e que não afeta pessoas e equipamentos energizados;
- 6.7.10. Garantir a detecção precoce de gases no ambiente incluindo a área situada sob o piso elevado utilizando detector VESDA, com sistema integrado de alarme monitorado e acompanhado em regime 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano;
- 6.7.11. Possuir sistema integrado aos túneis de ventilação do Data Center, de forma que em havendo o disparo de gás, o fluxo de ar é interrompido para a área do evento garantindo a extinção do incêndio sem afetar demais áreas do Data Center;
- 6.7.12. Em caso de sinistro, o disparo do gás deve ocorrer de forma automática, não havendo necessidade de intervenção humana;
- 6.7.13. O sistema de detecção precoce e combate a incêndio deverá possuir contrato de manutenção contemplando visitas preventivas e testes do sistema com o fabricante do mesmo no mínimo a cada 03 (três) meses;
- 6.7.14. A solução de ar-condicionado deve ser integrada a solução de combate a incêndio para que, em caso de incêndio, os dutos de ventilação sejam automaticamente fechados sem necessidade de intervenção humana;
- 6.7.15. Os equipamentos utilizados para prestação de serviços da CONTRATANTE deverão estar instalados em racks que trabalhem dentro de um sistema de Túnel Frio;
- 6.7.16. A climatização deverá ser composta por, no mínimo, segurança N+1 de unidades evaporadoras e, no mínimo, segurança N+1 de condensadoras externas ao edifício, interligadas por tubos de cobre isolados adequadamente;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 6.7.17. A climatização não deverá fazer troca de ar atmosférico. Tanto a sala de servidores quanto a sala de refrigeração deverão ser fechadas para que variações de temperatura, umidade e outros contaminantes não afetem os equipamentos dentro do Data Center;
- 6.7.18. Estar equipada com subestação elétrica própria e projetada para operar em média ou alta tensão, para atendimento aos requisitos de potência e alimentação elétrica adequadas e exclusivos para o Data Center;
- 6.7.19. Os sistemas devem ser equipados e protegidos por Nobreaks, bancos de baterias e geradores que funcionam automaticamente no caso de queda do fornecimento comercial;
- 6.7.20. Cada Nobreak deve possuir capacidade suficiente em regime N+1 para suportar todas as atividades do Data Center, incluindo as atividades previstas por este termo de referência;
- 6.7.21. Os nobreaks que atendem aos circuitos redundantes devem operar em regime Standalone, de maneira que os Nobreaks sejam completamente independentes entre si e sem risco de que a falha do primeiro se propague para o segundo;
- 6.7.22. O Data Center deve possuir sistema de geração elétrica à diesel próprio e redundante, que mantenha o ambiente em pleno funcionamento, durante todo o período de eventual corte de energia pela concessionária;
- 6.7.23. A autonomia do sistema de geração elétrica a diesel (grupo gerador) deverá ser de no mínimo 48 (quarenta e oito) horas sem reabastecimento de combustível.
- 6.7.24. Os geradores devem ser capazes de ser acionados para proteger o Data Center automaticamente não apenas em eventos de falta de energia, mas também quando algum parâmetro da concessionária estiver fora das especificações (frequência, tensão etc.);
- 6.7.25. No retorno da alimentação da concessionária, os grupos geradores devem ser capazes de sincronizarem sua alimentação e fazer a retirada da carga em rampa para evitar oscilações elétricas dentro do Data Center;
- 6.7.26. Os geradores e Nobreaks devem possuir contrato de manutenção contemplando visitas preventivas e testes do sistema com o fabricante dos mesmos com periodicidade mínima 1(uma) vez por mês;
- 6.7.27. O prédio da CONTRATADA deve atender a norma NBR 5410 para proteção de surto em todas as zonas.
- 6.7.28. Deve ser um sistema autônomo (AS) em relação à Internet por cadastro próprio, ou seja, possuir seus próprios blocos de IPv4, IPv6 e seu registro individual de ASN.
- 6.7.29. deverá possuir Solução Anti-DDoS, implementando proteção contra-ataques coordenados provenientes de múltiplos sistemas (comprometidos) e distribuídos geograficamente com o

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

intuito de gerar indisponibilidade dos serviços da CONTRATANTE através do esgotamento dos recursos.

- 6.7.30. Deverá ser fornecido o hardware que suporte todas as soluções presentes no Termo de Referência.
- 6.7.31. Possuir ambiente dedicado único e exclusivo para laboratório, onde seja possível reproduzir os incidentes e problemas da CONTRATANTE, sem que haja impacto na operação do Centro de Operações de Segurança e/ou da própria CONTRATANTE;
- 6.7.32. Possuir no Centro de Operações de Segurança processos consistentes e objetivos de monitoramento e detecção de ameaças, gestão de dispositivos, gestão de incidentes, inteligência de ameaças, investigação de ameaças e gestão de conformidade de segurança.
- 6.7.33. Possuir nativamente solução de SecOps para gerenciamento de incidentes de segurança da informação.
- 6.7.34. Deverá possuir processos implementados que garantam o cumprimento das normas e Lei Geral de Proteção de Dados. Tal exigência visa garantir controles rígidos e auditáveis de acesso físico e lógico às informações e monitoramento, além de comprovadamente contar com um comitê responsável pelos controles e adequações;

7. CONDIÇÕES GERAIS PARA PRESTAÇÃO DOS SERVIÇOS

- 7.1. Independentemente do grupo de serviço especificado, todas as soluções e/ou ferramentas utilizadas para prestação do serviço deverão obrigatoriamente seguir os requisitos, a saber:
 - 7.1.1. Deverá ser obrigatoriamente de propriedade da CONTRATADA ou licenciada para a CONTRATADA, não podendo ser do tipo *Open Source* (software livre).
 - 7.1.2. Deverá ser prestado por meio de solução provida através da nuvem do fabricante ou da CONTRATADA.
 - 7.1.3. Deve englobar o fornecimento de *Hardwares* e de *Softwares* necessários à execução dos serviços contratados durante o prazo de vigência do contrato, incluindo garantia, manutenção, atualização dos produtos e monitoramento de segurança em regime de 24 (vinte quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano;
 - 7.1.4. Os softwares ofertados devem ser instalados e atualizados em sua versão mais estável e estar cobertos por contratos de suporte e atualização de versão do fabricante durante a vigência do respectivo item de serviço. Da mesma maneira, os equipamentos fornecidos para a prestação dos serviços devem estar cobertos por contratos de garantia do fabricante;
 - 7.1.5. O conjunto de requisitos especificados para cada serviço pode ser atendido por meio de composição com outros equipamentos ou softwares utilizados no atendimento aos demais itens, de maneira integrada, desde que não implique alteração da topologia de rede ou na

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

exposição de ativos a riscos de segurança da informação, em termos de integridade, confidencialidade ou disponibilidade.

7.2. EQUIPE DE INTELIGENCIA DE AMEAÇAS

- 7.2.1. A contratada deverá contar com uma equipe de inteligência de ameaças dedicada a identificar as intenções, capacidades e, prioritariamente, as oportunidades usadas pelos criminosos através da coleta, normalização, correlação e análise de dados, transformando-os em inteligência e entregando ao CONTRATANTE relatórios periódicos, apresentando dados de mercado e o atual cenário do ambiente do CLIENTE.
- 7.2.2. Esses dados poderão ser utilizados para melhora na proteção, seja na atuação direta com a equipe de *Hunting* em novos casos de uso ou mantendo o time da CONTRATANTE informados, através de Boletins de Ameaças.
- 7.2.3. A CONTRATADA deverá possuir célula que entregue informações através de fontes de inteligências abertas e/ou próprias, compartilhando informações de inteligência através do MISP (*Malware Information Sharing Platform*), executando também a gestão dele através da equipe local, bem gerindo a integração entre o MISP da CONTRATANTE como da CONTRATADA.
- 7.2.4. A plataforma deverá ter capacidade de identificar vulnerabilidades em, no máximo, um dia após o surgimento desta, executar o correlacionamento com o inventário informado pela CONTRATANTE e informar via evento no MISP sobre os sistemas vulneráveis.
- 7.2.5. A CONTRATADA deverá possuir plataforma de inteligência que informe IoCs (Indicadores de Comprometimento) contendo, no mínimo, *Hashes* de binários maliciosos nos formatos MD5, SHA1, SHA256, *Filename*, domínios maliciosos, URLs maliciosas, bem como IPs maliciosos com geolocalização e pontuação de risco, reduzindo a possibilidade de falso positivo;
- 7.2.6. Deve possuir equipe de *Threat Intelligence* que execute Análise de Superfície, um trabalho que avalia o ambiente na perspectiva de um agente malicioso em busca de eventuais brechas utilizando o *Framework* OSINT (Inteligência de Fontes Abertas) com foco na identificação de superfície de ataque e as possíveis oportunidades na perspectiva de um agente malicioso.
- 7.2.7. Deve executar de forma recorrente a Análise de Superfície, no mínimo trimestralmente, utilizando especialistas de *Cyber Threat Intelligence* na execução de um *Assessment* interno e análise externa utilizando técnicas de OSINT, apresentando informações dos perímetros com objetivo de entregar relatório, apontando de forma prática como tratar cada ponto identificado e apresentar um *Score* qualitativo de maturidade para a CONTRATANTE.

7.3. PORTAL DE INDICADORES DE SERVIÇO

- 7.3.1. O portal de indicadores deverá ser disponibilizado à CONTRATANTE e contemplar, no mínimo, os requisitos abaixo:

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 7.3.2. A CONTRATADA deverá disponibilizar um sistema em modelo SaaS (do inglês *Software As Service*), denominado portal de indicadores, para consolidação dos dados gerados pelas soluções que compõem o objeto.
- 7.3.3. O portal deverá estar acessível à CONTRATADA via *Internet*, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, e 365 (trezentos e sessenta e cinco) dias por ano, de maneira segura utilizando protocolo de criptografia SSL.
- 7.3.4. A CONTRATANTE terá direito a criação de usuários ilimitados com a função de criação de perfis para cada usuário, disponibilizando assim visões diferentes para cada nível de acesso.
- 7.3.5. Deverá disponibilizar para os usuários da CONTRATANTE a função de mudança de visão gráfica a critério de cada usuário. Isso quer dizer que apesar de um gráfico estar disposto em modelo de barras, caso o usuário identifique uma melhor visualização do modelo gráfico em forma de pizza, o sistema deve oferecer tal funcionalidade ou opção.
- 7.3.6. O portal ainda deverá disponibilizar os seguintes modelos gráficos para os usuários:
- a) Gráfico do tipo Pizza;
 - b) Gráfico do tipo Barra;
 - c) Gráfico do tipo linha;
 - d) Gráfico do tipo área;
 - e) Gráfico do tipo funil;
 - f) Gráfico do tipo bolha.

7.3.7. INDICADORES DE RISCO – KRI:

- 7.3.7.1. Deverá ser exibido no portal a quantidade de Vulnerabilidades que estavam presentes na última auditoria realizada através de gráfico(s) com separação dos tipos/quantidades com a opção de “Drill Down”, possibilitando assim visualização de forma mais detalhada das vulnerabilidades listadas;
- 7.3.7.2. O portal deverá possuir recurso para filtrar apenas as vulnerabilidades relevantes, excluindo as de severidade média e/ou baixa.

7.3.8. INDICADORES DE META E PERFORMANCE – KGI e KPI:

- 7.3.8.1. O portal de indicadores deverá possuir relatório gráfico indicando tempo médio dos atendimentos dos incidentes por fase de Análise, contenção, erradicação e recuperação, possibilitando a filtragem por período:
- 7.3.8.2. Últimos 15 dias;
 - 7.3.8.3. Últimos 30 dias;
 - 7.3.8.4. Últimos 45 dias.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

7.3.9. Deverá possuir gráfico comparativo entre os primeiros e últimos 15 incidentes analisados dentro de período filtrado, mostrando numa linha de tempo qual foi o incidente com o tempo de atendimento menor, maior e o tempo médio.

7.3.10. Deverá ser possível a consulta deste gráfico para cada uma das fases de atendimento (análise, contenção, erradicação e recuperação).

7.4. INDICADORES POR CATEGORIA MITRE ATT&CK:

7.4.1. O Portal de indicadores deverá possuir gráfico que separe e classifique os incidentes de acordo com as categorias existentes na base de conhecimento do MITRE ATT&CK, sendo elas no mínimo:

- a) Initial Access;
- b) Execution;
- c) Persistence;
- d) Privilege Escalation;
- e) Defense Evasion;
- f) Lateral Movement;
- g) Collection;
- h) Command and Control;
- i) Exfiltration;
- j) Impact.

7.4.2. Todos os indicadores exibidos pelo portal, devem possuir a funcionalidade *Drill Down*, para que os usuários possam criar visualizações e filtros dos dados exibidos.

7.4.3. Todos os indicadores exibidos pelo portal devem ainda possuir funcionalidade de exibição dos dados gerados do gráfico de maneira tabular, a fim de que seja possível aferir os dados brutos.

7.4.4. O portal deve armazenar os dados durante o período mínimo de 1 (um) ano e deverá permitir a criação de filtros por períodos.

7.4.5. A qualquer tempo a CONTRATANTE poderá solicitar os dados brutos coletados das soluções que compõem o objeto contratado.

7.4.6. Os dados exibidos pelo portal devem representar o ambiente em tempo de execução e de forma automática (*Real Time*).

7.4.7. O portal deverá possibilitar customizar limiares dos serviços e eventos para gerar alarmes de acordo com o acordo de nível de serviço definido no presente termo de referência;

7.4.8. Deverá prover mecanismo para análise de risco e métricas de disponibilidade através de relatórios e *Dashboards* de todas as soluções que compõem o objeto.

7.5. SERVIÇO DE ACOMPANHAMENTO DE ENTREGAS

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 7.5.1. Deverá ser provido um serviço de acompanhamento de entregas através de reuniões de preferência virtuais para cadência do contrato de forma quinzenal.
- 7.5.2. **Entregável:** Ata de reunião
- 7.5.3. Deverá ser feito o acompanhamento periódico dos indicadores listados no contrato para antecipar desvios e corrigi-los antes que saiam das conformidades exigidas;
- 7.5.4. **Entregável:** Acompanhamento periódico a partir das ferramentas de registro de chamado ou medição (Portal de Indicadores);
- 7.5.5. **Entregável:** Checklist periódico dos entregáveis do projeto, conforme RFP, TR, proposta técnica e afins.
- 7.5.6. Deverá ser feito o acompanhamento do cronograma de faturamento mensal do contrato;
- 7.5.7. Deverá manter a matriz de comunicação atualizada dos dois lados do contrato – quem a CONTRATADA deve acionar e quem a CONTRATANTE deve acionar em casos específicos ou de escalção.
- 7.5.8. **Entregável:** Documento formal conforme formato pré-estabelecido.

7.6. SERVIÇO DE CONFORMIDADE DE DESEMPENHO CONTRATUAL

- 7.6.1. Deve ser provido serviço de conformidade de desempenho do contrato no qual deverão ser providas reuniões mensais entre a CONTRATANTE e a CONTRATADA com intuito de validação da satisfação referente aos serviços prestados.
- 7.6.2. Estas reuniões devem servir para identificação das necessidades da CONTRATANTE onde deverão ser apontados problemas recorrentes ou pontuais que estejam impactando a qualidade da execução do contrato.
- 7.6.3. Após essas reuniões deverão ser formulados planos de ações corretivos para cada área/serviço que não esteja cumprindo os padrões de qualidade exigidos no contrato.
- 7.6.4. O serviço deve ser executado por um especialista em resolução de crises ou temas críticos da CONTRATADA que funcione como moderador entre o time de entrega da CONTRATADA com os gestores do contrato da CONTRATANTE.
- 7.6.5. Entende-se como CRISE a atuação que é ou será baseada no desenvolvimento de um plano de ação para temas que gerem ônus imediato à CONTRATANTE, ônus direto e imediato à CONTRATADA, risco de exposição do ambiente da CONTRATANTE, risco de cancelamentos de contratos. Além disso, crises serão tratadas em conjunto com todas as áreas envolvidas, até a finalização do plano de ação de correção.
- 7.6.6. O especialista responsável por este serviço deve atuar também na escalção de temas não

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

críticos do dia a dia do contrato que não estejam sendo respondidos devidamente pela CONTRATADA.

- 7.6.7. Entende-se como **ESCALAÇÃO** problemas diários da CONTRATANTE em que a tratativa não foi eficaz e efetiva e/ou fora do tempo esperado/acordado, fazendo com que a CONTRATANTE eleve o tema para um nível hierárquico superior da CONTRATADA. Exemplos:
- 7.6.7.1. Falta de atuação de algum time específico;
 - 7.6.7.2. Falta de resposta à um e-mail, chamado e/ou questionamentos do CONTRATANTE;
 - 7.6.7.3. Falta de solução à um problema sinalizado pelo CONTRATANTE;
 - 7.6.7.4. Chamado em aberto, não atendido dentro do SLA acordado em contrato;
 - 7.6.7.5. Insatisfação da CONTRATANTE sobre um entregável como relatório, boletins, atuação/postura de recursos ou times;
 - 7.6.8. Este serviço deverá prover ainda um indicador denominado NPS (Net Promoter Score) que consiga metrificar a satisfação da CONTRATANTE em relação aos serviços prestados que estejam estipulados no contrato. Está métrica deverá seguir os padrões e fórmulas comuns de mercado e deverá ser atualizada e apresentada mensalmente aos gestores do contrato.
 - 7.6.9. Em quaisquer mudanças em que a CONTRATADA identifique possíveis impactos no ambiente, e/ou que necessite de alterações de configurações em servidores ou ferramentas que possuam amplo alcance deverão passar pelo processo de aprovação de RDM (Requisição de Mudança) da CONTRATANTE.

8. ESPECIFICAÇÃO DOS SERVIÇOS

8.1. SERVIÇOS DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS E RESPOSTA A INCIDENTES

- 8.1.1. Visa o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados a CONTRATANTE, através de fornecimento de serviços com capacidade de correlacionamento de eventos, para detecção de ameaças direcionadas a CONTRATADA para detecção de comportamento anômalo de serviços, que possam gerar eventos de segurança da informação, aos quais devem ser analisados, podendo estes serem transformados em um incidente de segurança da informação, obedecendo um processo cíclico e rigoroso de gestão de eventos.

8.1.2. SOBRE AS FERRAMENTAS A SEREM UTILIZADAS

- 8.1.2.1. Para execução deste serviço, a CONTRATADA deverá utilizar e ser capaz de fornecer, operar, sustentar e suportar soluções de monitoramento que atendam o descritivo técnico a seguir:

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 8.1.2.2. A plataforma utilizada deverá ter capacidade de operar com volumes massivos de dados em tempo real utilizando algoritmos de aprendizagem de máquina automática de máquina "Machine Learning" e deve contar com casos de uso para detectar ameaças avançadas.
- 8.1.2.3. A plataforma deverá possuir as características a seguir:
- 8.1.2.4. Extremamente escalável e tolerante a falhas, capaz de ingerir centenas de terabytes por dia e suportar a retenção de eventos de segurança por longo período.
- 8.1.2.5. Junte-se a eventos ao longo do tempo usando modelos Kill Chain para a análise de eventos de maior risco.
- 8.1.2.6. Permitir o hunting rápido de ameaças por meio da pesquisa em linguagem natural.
- 8.1.2.6.1. A solução deve estar classificada como líder no quadrante mágico de "Security Information and Event Management" pelo menos no último ou penúltimo ano;
- 8.1.2.6.2. A solução deve ter recursos de "Multi-tenant";
- 8.1.2.6.3. Deve ser do tipo Nuvem em Software como um modo de Serviço e ter as certificações SOC 2 TYPE II e ISO 27001.
- 8.1.2.6.4. Deve garantir retenção dos logs conforme arquitetura abaixo:
- a) 7 dias hot retention;
 - b) 90 dias warm retention;
 - c) 365 dias cold retention.
- 8.1.2.6.5. Deve ter alta disponibilidade e mecanismos de recuperação de desastres;
- 8.1.2.6.6. Deve permitir a filtragem e compressão de dados seletivos em até 90% no ponto de coleta;
- 8.1.2.6.7. Deve permitir o gerenciamento da largura de banda para a transmissão de dados entre os coletores e os servidores de gerenciamento;
- 8.1.2.6.8. Deve executar o armazenamento em cache local e/ou em buffer nos coletores para garantir que nenhum dado seja perdido em trânsito no caso de um problema de rede ou um pico no volume do evento;
- 8.1.2.6.9. Deve oferecer suporte ao mascaramento de dados por meio de controles de acesso granulares baseados em funções, para ofuscar qualquer informação de usuário potencialmente sensível na camada de interface do usuário;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 8.1.2.6.10. Deve suportar controle de acesso baseado em função granular (RBAC) com suporte a administração delegada, tanto para as funcionalidades na interface do usuário quanto acesso aos dados e configurações;
- 8.1.2.6.11. Deve incluir uma ferramenta de Security Datalake baseada em bigdata em uma arquitetura aberta e escalável e com capacidade de coletar e reter dados por períodos estabelecidos para fins de conformidade e investigação;
- 8.1.2.6.12. Deve ter uma instância de homologação para testes que permita isolar, do ambiente de produção, novas integrações, novos desenvolvimentos de conteúdos e novos analisadores;
- 8.1.2.6.13. A solução deve atender as seguintes características:
- 8.1.2.6.13.1. Deve oferecer suporte a integração com mais de 500 fontes de eventos usando métodos de syslog, formatos de log estruturados (CEF, LEEF, MEF, JSON, XML), arquivos, bancos de dados (conexão JDBC), conexão API (AWS, Azure, Box, Crowdstrike, Google Report, Netskope, SVN, Salesforce, Splunk, QRadar, Netwitness, Office 365, Okta, Proofpoint, Sumologic, Workday, entre outros), WMI, consultas LDAP/LDAPS, dados e fluxo (Netflow, sFlow, jFlow), Hadoop, Registros não estruturados (Regex), agentes de terceiros (snare);
- 8.1.2.6.14. Deve permitir a integração com diferentes tipos de fontes de dados, como dados de identidade, logs de atividades / transações, logs de eventos de segurança, fluxos de rede, log de aplicativos / plataformas de nuvem, permissões de acesso, fontes de inteligência de ameaças, dados não estruturados e metadados de ativos;
- 8.1.2.6.15. Deve permitir conexão a sistemas externos de gerenciamento de identidade, como Active Directory / LDAP ou soluções de IAM (gestão de identidade), como Aveksa/Sailpoint, sistemas de RH, como Peoplesoft/Workday, para realizar o enriquecimento contextual de eventos adicionando identidade do usuário;
- 8.1.2.6.16. Deve ser capaz de se conectar nativamente através de APIs ou outros meios com serviços em nuvem como Salesforce, Amazon Web Services S3 e Cloudtrail, BOX, Microsoft Azure, Office 365, Google Apps, Google Cloud, Netskop, ServiceNow, entre outros.
- 8.1.2.6.17. Deve ter uma interface de usuário que permita modificar conectores, analisadores (parsers) existentes ou construir novos analisadores (parsers) na mesma interface de usuário;
- 8.1.2.6.18. Deve ter conectores, analisadores (parsers) pré-configurados, prontos para uso, mas que possam ser modificados conforme necessário. A análise, normalização e categorização dos coletores devem ser totalmente personalizáveis na interface

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

do usuário.

- 8.1.2.6.19. Deve ter uma API RESTful de serviços para integração bidirecional com outras tecnologias;
- 8.1.2.6.20. Deve fornecer integração com pelo menos 5 fontes de inteligência de ameaças incluídas no valor do serviço ofertado;
- 8.1.2.6.21. Deve realizar o enriquecimento dos eventos com dados contextuais sobre eventos no momento da captura e ingestão de dados adicionando aos eventos:
- a) Identidade do usuário;
 - b) Contexto de negócios;
 - c) Metadados de ativos;
 - d) Informações de rede;
 - e) Localização Geográfica;
 - f) Dados de inteligência de ameaças;
- 8.1.2.6.22. Deve enriquecer eventos em tempo real com contexto de usuário e entidade. Os dados ricos podem fornecer atributos de contexto que podem ser usados para perfis comportamentais, comparações de pares, pesquisas e investigações;
- 8.1.2.6.23. Deve detectar ameaças cibernéticas e internas avançadas (insider threat) usando aprendizado de máquina para criar perfis e linhas de base de comportamento de usuários e entidades;
- 8.1.2.6.24. Deve ter conteúdo pré-empacotado de casos de uso e modelos de ameaças prontos para uso para detecção avançada de ameaças, como:
- a) Detecção de ameaças internas (insider threat) utilizando técnicas de aprendizagem de máquina;
 - b) Detecção de ameaças cibernéticas (cyber threat) utilizando técnicas de aprendizagem de máquina;
 - c) Detecção de ameaças na nuvem (cloud threat) utilizando técnicas de aprendizagem de máquina;
- 8.1.2.6.25. Deve fornecer recursos abrangentes para modelar e ajustar a pontuação de risco com base no perfil do usuário e/ou entidade, gravidade da ameaça e sequência/combinção de eventos que ocorrem durante um período;
- 8.1.2.6.26. Deve permitir a modelagem de risco a partir da interface do usuário de acordo com as prioridades da organização;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 8.1.2.6.27. Deve ter modelos de ameaças que permitam agrupar eventos realizados por um usuário ou entidade que duram dias, semanas, meses e assim por diante. Essas atividades devem ser exibidas como uma cadeia de eliminação com cada evento categorizado em estágios predefinidos.
- 8.1.2.6.28. Deve ter algoritmos preditivos para identificar usuários de risco (por exemplo, usuários prestes a deixar a organização);
- 8.1.2.6.29. Deve fornecer análises para diferentes tipos de anomalias, como relacionadas ao tempo, volume de transferência de dados, origem do evento relacionado, destino do evento relacionado, anomalias por usuário e grupo de pares, anomalias relacionadas a localização geográfica / velocidade terrestre, bem como rastrear usuários ou outras entidades nas listas de observação;
- 8.1.2.6.30. Deve ter algoritmos de aprendizagem não supervisionados para analisar eventos atuais e históricos e determinar associações, para estabelecer padrões de comportamento da atividade do usuário em cada fonte de evento por dia, semana, mês, hora do dia e dia da semana. Qualquer desvio do padrão regular deve ser marcado como uma anomalia;
- 8.1.2.6.31. Deve ter algoritmos de aprendizagem supervisionados para detectar ameaças de malware avançadas, como DGA, ataques de phishing/spam e muito mais;
- 8.1.2.6.32. Deve ter técnicas de análise baseadas pares para detectar usuários que estão começando a se comportar de maneira diferente dos pares, traçando o perfil do comportamento de diferentes usuários no grupo de pares e, em seguida, comparando as transações do usuário com a dos pares;
- 8.1.2.6.33. Deve haver técnicas de análise de raridade de eventos pelas quais atividades suspeitas que não foram vistas antes possam ser identificadas;
- 8.1.2.6.34. Deve ter técnicas de análise de comportamento por enumeração que permita criar linhas de base de eventos do mesmo tipo e procurar qualquer desvio do normal;
- 8.1.2.6.35. Deve ter técnicas de análise de tráfego para identificar padrões de beaconing, agentes de usuários incomuns, conexões com URLs incomuns, conexões com domínios DGA, etc;
- 8.1.2.6.36. Deve fornecer a capacidade de definir políticas baseadas em regras para detectar ameaças conhecidas. Essas ameaças conhecidas devem ser usadas como intensificadores de risco e combinadas com as verificações “não assinadas” nos modelos de ameaças;
- 8.1.2.6.37. Deve haver modelagem de ameaças que permita a identificação de ameaças compostas, que se observadas isoladamente podem ser de baixo risco, porém,

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

quando combinadas, são indicativas de um evento de alto risco;

- 8.1.2.6.38. Deve reduzir o número de falsos positivos aplicando recursos avançados de aprendizado de máquina para aprender o que é normal e o que não é normal no ambiente monitorado;
- 8.1.2.6.39. Deve ter relatórios de ameaças que forneçam visibilidade da postura de segurança cibernética. Por exemplo: usuários de alto risco, ativos de alto risco, principais ameaças, principais IPs maliciosas, etc;
- 8.1.2.6.40. Deve ter relatórios que forneçam visibilidade sobre as operações de segurança. Por exemplo, para dispositivos VPN, os relatórios devem incluir as melhores sessões de VPN por duração, os principais eventos de saída de dados, a distribuição dos eventos de login por geografia, as principais tentativas de login com falha e assim por diante;
- 8.1.2.6.41. Deve ter relatórios de conformidade alinhados com requisitos de conformidade específicos, como PCI, SOX, HIPPA, GDPR, ISO27002, etc;
- 8.1.2.6.42. Deve ter relatórios de resumo executivo de violações, incidentes e operações;
- 8.1.2.6.43. Deve ter relatórios sobre a atividade do usuário;
- 8.1.2.6.44. Deve permitir que os dados sejam exibidos com diferentes tipos de gráficos: gráfico de linhas, gráfico de barras, gráfico de pizza, mapa geográfico, tabelas, gráfico empilhados, gráfico N principais, gráficos de bolhas, gráficos de relacionamento de origem e destino;
- 8.1.2.6.45. Deve permitir a visualização de dados através de links que permitam vincular qualquer conjunto de atributos e visualização a relação entre eles;
- 8.1.2.6.46. O serviço deve possuir solução para análise de artefatos maliciosos que minimamente contemple as funcionalidades a seguir:
 - a) Analisar mais de 1000 indicadores comportamentais de um artefato;
 - b) Realizar análise estatística e dinâmica para avaliar se o artefato é malicioso ou não;
 - c) Deve suportar a análise dos artefatos BAT, CHM, DLL, ISO, HTA, HWP, JAR, JS, JSE, JTD, LNK, MSI, MHTML, documentos do Microsoft Office, EXE, PE32, PDF, VBE, URLs, WSF, XML e ZIP;

8.1.3. PROCESSOS A SEREM APLICADOS

8.1.3.1. PROCESSO DE MONITORAMENTO, DETECÇÃO E RESPOSTA

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 8.1.3.1.1. A CONTRATADA será responsável por implantar, operar e suportar toda a plataforma ofertada;
- 8.1.3.1.2. A fim de balizar todo o processo de monitoramento de ataques cibernéticos da CONTRATANTE, e influenciado pelos principais frameworks de boas práticas de serviços de segurança da informação, deverá ser desenhado/revisado em conjunto com a CONTRATANTE, o processo de resposta a incidentes focado em cibersegurança escopo desse contrato, que seja aderente as características específicas do ambiente da CONTRATANTE.
- 8.1.3.1.3. Após a definição/revisão e escrita da política de respostas a incidentes de cibersegurança, para início da implementação dos processos, deverá haver o aceite formal da CONTRATANTE.
- 8.1.3.1.4. É sabido que para o sucesso de um monitoramento de ataques cibernético, a primeira definição se deve a que tipo de ocorrência de eventos de segurança, se deseja detectar e tomar algum tipo de ação, logo será de responsabilidade da CONTRATADA como primeiro passo deste processo, a definição de linha de base de eventos monitorados.
- 8.1.3.1.5. Tal definição de linha de base de eventos de segurança monitorados, não deve ser tomada de forma unilateral pela CONTRATADA. A CONTRATANTE deverá participar ativamente no processo de construção de forma consultiva. Porém, se ratifica que é de responsabilidade da CONTRATADA a definição, e colocar em operação tal linha de base.
- 8.1.3.1.6. Espera-se que a linha de base de eventos de segurança monitorados, seja revista de forma mensal, contudo, não se limitando a este tempo, pois todos os dias novos ataques são projetados no mundo, e se espera que a CONTRATADA tome ciência destes ataques, e por sua vez atualize a linha de base, para que em um cenário onde estes novos ataques sejam direcionados a CONTRATANTE, sejam detectados através dos serviços em questão.
- 8.1.3.1.7. O produto de um evento é a correlação dos logs gerados pelos itens de configurações do parque da CONTRATANTE. Uma vez definida a linha de base de eventos, será também de responsabilidade da CONTRATADA avaliar se todos os insumos para a correta geração do evento, estão sendo enviados corretamente para a ferramenta.
- 8.1.3.1.8. Caso a CONTRATADA identifique a ausência dos insumos (eventos) a ser gerado por um item de configuração, será de reponsabilidade da CONTRATADA a correção e/ou habilitação de tal insumo dos itens de configuração descritos no tópico AMBIENTE TECNOLÓGICO DA CONTRATANTE (HARDWARE E SOFTWARE). Caso o item de configuração não pertencer ao objeto contratado, porém necessário para a correta geração do evento, deverá a CONTRATADA solicitar a CONTRATANTE a correção e/ou habilitação de tal insumo no item de

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

configuração em questão.

8.1.3.1.9. Dar-se-á então o passo de classificação do evento, também de responsabilidade da CONTRATADA. O grupo de monitoramento de ataques da CONTRATADA deve focar as ações nos eventos que são significativos. Logo, tal grupo deve analisar todos os eventos apresentados, classificando-os nos seguintes grupos, a saber:

- 8.1.3.1.9.1. Eventos de Informação: Estes eventos não requerem qualquer ação. São usados para fazer verificação de funcionalidade dos itens de configuração de segurança. Ou seja, tem por objetivo puro e simples, identificar se as ferramentas e soluções estão funcionando dentro do esperado. Estes eventos são também úteis para gerar estatísticas como, por exemplo, porcentagem de hosts com a última vacina de antivírus do dia.
- 8.1.3.1.9.2. Eventos de Aviso: Este grupo de eventos deve ser utilizado quando existe algum comportamento anômalo, se comparado a linha de base de operação padrão do ambiente (serviço ou solução), porém, ainda não gerou algum tipo de impacto ao ambiente (serviço ou solução) da CONTRATANTE, como por exemplo fictício: É esperado que exista 1.000 (mil) ataques do tipo port scan bloqueados pelo firewall, porém, na última hora, este número passou para 10.000 (dez mil) ataques, todavia, o firewall ainda continua bloqueando sem que haja degradação da performance do ambiente (serviço, tráfego e/ou solução).
- 8.1.3.1.9.3. Eventos de Exceção: Estes eventos são aqueles que sugere que os pilares de segurança da informação (confidencialidade, integridade e conformidade), foram impactados como, por exemplo: Uma infecção gerada por um malware do tipo ransomware, onde a mesma não tenha sido bloqueada pela solução de antivírus da CONTRATANTE. Este é o único tipo de evento que pode iniciar o processo de resposta a incidente de segurança, descrito no tópico, do presente termo de referência.
- 8.1.3.1.9.4. Uma vez classificado o evento, se inicia o passo de resposta ao mesmo, que também é de responsabilidade da CONTRATADA. As respostas a serem dadas a cada tipo de incidentes, serão baseadas na política de resposta a incidentes escrita previamente conforme descrito no presente termo.
- 8.1.3.1.9.5. Durante a fase de escrita e/ou definição dos processos a serem seguidos, deverá ser informado quais os respectivos tipos de ações para no mínimo os seguintes tipos de eventos:
- 8.1.3.1.9.6. Informacional;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 8.1.3.1.9.7. Aviso;
 8.1.3.1.9.8. Exceção;

8.1.3.1.10. Importante ressaltar que todo o processo de tratamento do evento, independente de qual fase e/ou status, deve ser registrado no módulo de tratamento de eventos da ferramenta. Também é responsabilidade da CONTRATADA a segurança dos eventos, e fica expressamente proibido a remoção de qualquer evento, independentemente de sua classificação e fase de tratamento, sem a autorização da contratante.

8.1.3.1.11. Deverá em conjunto com a CONTRATANTE, ser criado playbooks de resposta a incidentes.

8.1.4. GRUPO TÉCNICO DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS

- 8.1.4.1. Através do seu centro de operação de segurança, a CONTRATADA deverá manter uma torre de operação denominada GRUPO DE MONITORAMENTO DE ATAQUES, com objetivo e foco de trabalhar no processo de monitoramento de ataques cibernéticos.
- 8.1.4.2. Este grupo deverá ser exclusivo para trabalhar no serviço em questão, não podem os profissionais pertencentes a este grupo serem compartilhados e/ou atuarem, com os demais serviços descritos no objeto do presente termo de referência.
- 8.1.4.3. Todos os profissionais que integram GRUPO DE MONITORAMENTO DE ATAQUES, devem obrigatoriamente compor o quadro permanente de colaboradores da CONTRATADA em regime de trabalho CLT (Consolidação das Leis do Trabalho) ou contrato de prestação de serviços firmados diretamente entre esses profissionais e a CONTRATADA, sendo proibida a terceirização ou subcontratação de tal serviço.
- 8.1.4.4. Além dos profissionais que deverão ficar dedicados ao contrato conforme informado previamente no presente termo de referência o dimensionamento é de responsabilidade da CONTRATADA quantificar o número adequado de profissionais para a entrega de tal serviço, sem que haja impacto no acordo de nível de serviço estabelecido no tópico ACORDO DE NÍVEIS DE SERVIÇO do presente termo de referência.
- 8.1.4.5. A fim de garantir que os profissionais envolvidos tenham conhecimento e habilidade para executar o processo de monitoramento de ataques cibernéticos da CONTRATANTE, a CONTRATADA deverá, obrigatoriamente, compor o GRUPO DE MONITORAMENTO DE ATAQUES, com ao menos 01 (um) perfil de cada profissional que segue descrito abaixo:

Perfis	Certificações	Descrição
Analista de Segurança I	- CompTIA Security+ - CompTIA CySA+ - e/ou Certified Ethical Hacker	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

	Certificação em pelo menos uma das soluções escolhidas para atender o tópico SOBRE AS FERRAMENTAS A SEREM UTILIZADAS	Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.
Analista de Segurança II	- CompTIA Security+ e/ou - CompTIA CySA+ e/ou - Certified Ethical Hacker	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de SIEM e ATD. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.

Tabela 2 - Certificações e qualificações do Grupo de Monitoramento de Ataques

8.1.4.6. Não existe restrição ou limite para acúmulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos no GRUPO DE MONITORAMENTO DE ATAQUES, porém, conforme já foi mencionado neste termo de referência, este(s) deve(m) compor única e exclusivamente o time denominado GRUPO DE MONITORAMENTO DE ATAQUES.

8.1.4.7. ENTREGAS A SEREM REALIZADAS

8.1.4.7.1. Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, o CONTRATANTE definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue de forma on line e em tempo de execução, através do portal de indicadores descrito no tópico de condições gerais para prestação do serviço deste termo de referência, a saber:

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Quantitativo de eventos correlacionados	Soma de eventos correlacionados	Eventos correlacionados	Eventos correlacionados	Número total de eventos correlacionados
Quantitativo de incidentes abertos	Soma de incidentes abertos	Incidentes abertos	Incidentes	Número total de incidentes abertos
Quantitativo de solicitações por grupo de tecnologia	Soma de solicitações relacionadas aos grupos de tecnologia	Solicitações relacionadas aos grupos de tecnologia	Solicitações	Número total de solicitações relacionadas por grupo de tecnologia
Quantitativo de regras de correlacionamento	Soma do número de regras de correlacionamento	Regras de correlacionamento	Regras de correlacionamento	Número total de regras de correlacionamento
TOP 10 – Regras de correlacionamento	Soma do número de eventos correlacionados por regra de correlacionamento	Eventos correlacionados	Regra de correlacionamento	TOP 10 do número de eventos correlacionados por regra de correlacionamento
TOP 10 – IP de destino de regras de correlacionamento	Soma do número de eventos correlacionados por IP de destino	Eventos correlacionados por IP de destino	IP de destino	TOP do número de eventos correlacionados por IP de destino
TOP 10 – Regras de correlacionamento por país de origem	Soma do número de eventos correlacionados por país de origem	Eventos correlacionados por país de origem	País de origem	TOP do número de eventos correlacionados por país de origem
TOP 10 – Tipos de ataques	Soma do número de ataques correlacionados por tipo de ataque	Eventos correlacionados por ataque	Ataques	TOP 10 por tipo de ataque

Tabela 3 - Indicadores Estratégicos de Monitoramento de Ataques Cibernéticos

9. SERVIÇO DE GESTÃO DE VULNERABILIDADES PARA 300 (TREZENTOS) ATIVOS

9.1. Tem por objetivo de forma proativa e recorrente, identificar possíveis vulnerabilidades de segurança da informação, na infraestrutura e aplicações do CONTRATANTE, identificando proativamente as vulnerabilidades de aplicações que seriam vetores de ataques, e tornando-as elegíveis de blindagem contra a exploração das vulnerabilidades identificadas afim de evitar que ataques cibernéticos direcionados ao CONTRATANTE, obtenha sucesso explorando tais vulnerabilidades já conhecidas.

9.2. SOBRE AS FERRAMENTAS A SEREM UTILIZADAS

9.2.1. ESPECIFICAÇÕES GERAIS

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 9.2.1.1. A solução deve realizar varreduras (*Scans*) de vulnerabilidades, avaliação de configuração e conformidade (*Baseline e Compliance*);
- 9.2.1.2. A solução deve possuir recurso de varredura ativa, onde o *Scanner* comunica-se com os alvos (ativos) através da rede;
- 9.2.1.3. A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT;
- 9.2.1.4. A solução deve ser licenciada pelo número de endereços IP ou dispositivos (*Assets*);
- 9.2.1.5. A solução deve fornecer um modelo de armazenamento integrado que não dependa de um banco de dados externos ou de terceiros;
- 9.2.1.6. Caso a solução dependa de banco de dados de terceiros, todas as licenças deverão ser fornecidas pela CONTRATADA.
- 9.2.1.7. A solução deverá suportar API (*Application Programming Interface*) baseada em REST (*Representational State Transfer*) para automação de processos e integração com aplicações terceiras.
- 9.2.1.8. A solução deve possuir integração via API no mínimo para as seguintes linguagens: *Python, Powershell, Ruby, Javascript, Java, Swift e PHP*;
- 9.2.1.9. A solução deve possuir métodos de consulta via API e envio, tais como: HTTP METHOD (POST, GET, PUT AND DELETE);
- 9.2.1.10. A solução deve incluir a opção para agentes instalados e licenciados em estações de trabalho e servidores para varredura diretamente no sistema operacional;
- 9.2.1.11. Tais agentes devem ser gerenciados pela mesma interface/console da plataforma de gestão de vulnerabilidades;
- 9.2.1.12. A solução deve permitir o agrupamento de *Scanners* para facilitar o gerenciamento e aplicação de políticas;
- 9.2.1.13. A solução deve realizar a varredura tanto de dispositivos na rede interna, dispositivos expostos a demais redes externas, tanto quanto dispositivos em nuvens públicas como Azure, AWS ou GCP;
- 9.2.1.14. O escaneamento para os dispositivos expostos deve ser realizados através de SCANS (ENGINE) do próprio fabricante alocados no Brasil;
- 9.2.1.15. Os Scanners e sensores agentes deverão ser gerenciados por uma única plataforma, de maneira centralizada;
- 9.2.1.16. O acesso a console de gerenciamento deve ser fornecida para pelo menos 10 usuários

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

simultâneos;

- 9.2.1.17. A solução deve ser capaz de se integrar e disponibilizar insumos para soluções de correlação de eventos externa (SIEM);
- 9.2.1.18. A solução deve apresentar, para cada vulnerabilidade encontrada, a descrição e passos que devem ser tomados para correção;
- 9.2.1.19. A solução deve apresentar, para cada vulnerabilidade encontrada, evidências da vulnerabilidade através de saídas das verificações (Outputs);
- 9.2.1.20. A solução deve fornecer controle de acesso baseado em função (RBAC- Role Based Access Control) para controlar o acesso do usuário a conjuntos de dados e funcionalidades;
- 9.2.1.21. A solução deve ser capaz de definir e gerenciar grupos de usuários, incluindo limitação de funções de varreduras e acesso a relatórios e Dashboards;
- 9.2.1.22. A solução deve ter a capacidade de excluir determinados endereços IP do escopo de qualquer varredura ou Scan;
- 9.2.1.23. A solução deve criptografar todos resultados de varreduras obtidos e informações inseridas tanto em descanso quanto em trânsito;
- 9.2.1.24. A solução deve suportar métodos de autenticação usando bases de autenticação local, e SAML (Security Assertion Markup Language) para uso de SSO (Single Sign-On);
- 9.2.1.25. A solução deve ser capaz de orquestrar Scanners ilimitados dentro da infraestrutura;
- 9.2.1.26. A solução não deve impor nenhum limite de quantidade de Scanners implementados dentro da infraestrutura;
- 9.2.1.27. A solução deverá possuir sistema de alertas para informar a disponibilidade de resultados dos escaneamentos através de Email;
- 9.2.1.28. A solução deve oferecer capacidade de configuração dinâmica de grupos de ativos através de no mínimo as seguintes características:
- 9.2.1.28.1. Sistema Operacional, Endereço IP, DNS, NetBIOS Host, MAC, AWS Instance Type, AWS EC2 Name, Software instalado, Azure VM ID, AWS Region, Google Cloud Instance ID, Azure Resource ID, Ativos avaliados;
- 9.2.2. Dos requisitos e relatórios e painéis gerenciais
- 9.2.2.1. A solução deverá possuir painéis gerenciais (Dashboards) pré-definidos para rápida visualização dos resultados, permitindo ainda a criação de painéis personalizados;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 9.2.2.2. Os painéis gerenciais deverão ser apresentados em diversos formatos, incluindo gráficos e tabelas, possibilitando a exibição de informações em diferentes níveis de detalhamento;
- 9.2.2.3. Os relatórios devem ser disponibilizados sob demanda no console de gerência da solução;
- 9.2.2.4. Os relatórios devem conter informações da vulnerabilidade, severidade, se existe um Exploit disponível e informações do ativo;
- 9.2.2.5. A solução deve permitir a customização de Dashboards/relatórios;
- 9.2.2.6. A solução deve concentrar todos os relatórios na plataforma central de gerenciamento, não sendo aceitas soluções fragmentadas;
- 9.2.2.7. A solução deve ser capaz de produzir relatórios, pelo menos, nos seguintes formatos: HTML, PDF e CSV;
- 9.2.2.8. A solução deve possibilitar a criação de relatórios baseado nos seguintes alvos: Todos os ativos e Alvos específicos;
- 9.2.2.9. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável);
- 9.2.2.10. A solução deve suportar o envio automático de relatórios para destinatários específicos;
- 9.2.2.11. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;
- 9.2.2.12. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;
- 9.2.3. Das varreduras
 - 9.2.3.1. A solução deve realizar varreduras em uma variedade de sistemas operacionais, incluindo, no mínimo, Windows, Linux e Mac OS, bem como Appliances virtuais;
 - 9.2.3.2. A solução deve suportar varredura com e sem agente, de maneira ativa e passiva, distribuídas em diferentes localidades e regiões e gerenciar todos por uma console central;
 - 9.2.3.3. A solução deve fornecer agentes instaláveis em sistemas operacionais distintos para monitoramento contínuo de vulnerabilidades;
 - 9.2.3.4. Tais agentes devem realizar conexões para o sistema gerenciamento através de protocolo seguro;
 - 9.2.3.5. A solução deve ser configurável para permitir a otimização das configurações de varredura;
 - 9.2.3.6. A solução deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 9.2.3.7. A solução deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;
- 9.2.3.8. A solução deve se integrar com solução de gerenciamento de acessos privilegiados para autenticação nos dispositivos, no mínimo, os seguintes:
- 9.2.3.8.1. CyberArk;
 - 9.2.3.8.2. BeyondTrust;
 - 9.2.3.8.3. Thycotic;
 - 9.2.3.8.4. Centrify;
- 9.2.3.9. A solução deve suportar o agendamento de *Scans* personalizados, incluindo a capacidade de executar varreduras em tempos designados, com frequência pré-determinada;
- 9.2.3.10. A solução deve ser capaz de identificar novos *hosts* no ambiente sem a necessidade de *Scan*;
- 9.2.3.11. A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;
- 9.2.3.12. A solução deve ser capaz de realizar em tempo real a descoberta de vulnerabilidades nas seguintes tecnologias:
- 9.2.3.12.1. Cloud Services;
 - 9.2.3.12.2. Data Leakage;
 - 9.2.3.12.3. Database;
 - 9.2.3.12.4. IoT;
 - 9.2.3.12.5. Mobile Devices;
 - 9.2.3.12.6. Operating System;
 - 9.2.3.12.7. Peer-To-Peer;
 - 9.2.3.12.8. Web Servers;
 - 9.2.3.12.9. Web Clients.
- 9.2.3.13. A solução deve ser capaz de identificar a comunicação de malwares na rede de forma passiva;
- 9.2.3.14. A solução deve, em tempo real, detectar Logins e Downloads de arquivos em um compartilhamento de rede;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

9.2.4. Da análise e priorização de vulnerabilidades

9.2.4.1. A solução deve ser capaz de exibir ambos severidade e pontuação, com base em CVSS (Common Vulnerability Scoring System) e inteligência de ameaças;

9.2.4.2. A solução deve utilizar sistema de pontuação e priorização das vulnerabilidades que utilize no mínimo:

9.2.4.2.1. CVSS Impact Score;

9.2.4.2.2. Idade da Vulnerabilidade;

9.2.4.2.3. Maturidade de códigos de exploração da vulnerabilidade encontrada;

9.2.4.2.4. Frequência de uso da vulnerabilidade em ataques e campanhas atuais;

9.2.4.2.5. Disponibilidade do código de exploração da vulnerabilidade;

9.2.4.2.6. Presença de módulos de exploração de vulnerabilidade em Frameworks automatizados de exploração de vulnerabilidades como CANVAS, Metasploit e Core Impact;

9.2.4.2.7. Popularidade da vulnerabilidade em fóruns e comunicações na *Darkweb*;

9.2.4.2.8. O mecanismo de priorização deve ser sujeito a modificações e atualizações diárias com base em inteligência de ameaças e observação de tendências na *Internet*;

9.2.5. Da Análise de Risco do Ambiente

9.2.5.1. A solução deve gerar um Score que combine dados de vulnerabilidades com a criticidade dos ativos do ambiente computacional;

9.2.5.2. O Score deve ser gerado automaticamente por meio de algoritmos de inteligência artificial (Machine Learning) e deve calcular a probabilidade de exploração de uma determinada vulnerabilidade;

9.2.5.3. Deve ser capaz de calcular a criticidade dos ativos da organização;

9.2.5.4. A solução deve ser capaz de realizar um Benchmark no ambiente da CONTRATANTE comparando sua maturidade com outras organizações do mesmo setor;

9.2.5.5. A solução deve prover visão sobre quais ações de remediação reduzem o maior nível de risco do ambiente;

9.2.5.6. A solução deve também permitir a visualização de ações de remediação agregadas para visão consolidada de redução de risco;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 9.2.5.7. Deve permitir modificar a qualquer momento o tipo de indústria para comparação. Ex: Mudar de Setor Público para Mercado Financeiro;
- 9.2.5.8. Deve fornecer uma lista com as principais recomendações para o ambiente com foco na redução da exposição cibernética da organização;
- 9.2.5.9. A solução deve gerar uma pontuação para cada um dos ativos onde é levado em conta as vulnerabilidades presentes naquele ativo assim como a classificação do ativo na rede (peso do ativo);
- 9.2.5.10. A solução deve gerar uma pontuação global referente a exposição cibernética da organização baseado nas pontuações de cada um dos ativos;
- 9.2.5.11. A solução deve oferecer uma capacidade de comparação (Benchmarking) da pontuação referente a exposição cibernética com outros Players da mesma indústria assim como outras empresas do mercado;
- 9.2.5.12. A solução deve permitir um acompanhamento histórico do nível de exposição da organização;
- 9.2.5.13. Permitir realizar alterações na classificação dos ativos (atribuição de pesos diferentes) podendo sobrescrever a classificação atribuída automaticamente pela solução;
- 9.2.5.14. A solução deverá apresentar indicadores específicos referentes a remediação, possuindo no mínimo informações referentes ao tempo entre remediação e o tempo o qual a vulnerabilidade foi descoberta no ambiente, tempo entre a remediação e a data de publicação da vulnerabilidade, quantidade média de vulnerabilidades críticas por ativo e a comparação da quantidade de vulnerabilidades corrigidas por criticidade;
- 9.2.5.15. A solução deve permitir a segregação lógica entre áreas distintas da empresa a fim de obter a pontuação referente exposição cibernética por área;
- 9.2.6. Da descoberta de Ativos:
- 9.2.6.1. A solução deve ser capaz de realizar escaneamento de descoberta de rede utilizando os seguintes critérios como alvo: IP, CIRD e Range;
- 9.2.6.2. A solução deve disponibilizar modelos de escaneamento de descoberta, ajustável, com os seguintes tipos de scan:
- 9.2.6.2.1. Enumeração de Hosts;
 - 9.2.6.2.2. Identificação de Sistema Operacional (SO);
 - 9.2.6.2.3. Port Scan (Portas comuns);
 - 9.2.6.2.4. Port Scan (Todas as portas);

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

9.2.6.2.5. Customizado;

9.2.6.3. A solução deve permitir realizar escaneamento de descoberta customizado podendo ser parametrizado de acordo com a necessidade;

9.2.6.4. A parametrização do escaneamento de descoberta deve, no mínimo, conter os seguintes requisitos:

9.2.6.4.1. Descoberta de Host;

9.2.6.4.2. Ping o host remoto;

9.2.6.4.3. Usar descoberta rápida;

9.2.6.4.4. Métodos de ping;

9.2.6.4.4.1. ARP;

9.2.6.4.4.2. TCP;

9.2.6.4.4.3. ICMP;

9.2.6.4.4.4. UDP;

9.2.6.4.5. Escaneamento de descoberta em redes de impressora;

9.2.6.4.6. Escaneamento em redes Novell;

9.2.6.4.7. Tecnologia de Wake-on-LAN;

9.2.6.5. Port Scanning:

9.2.6.5.1. Portas;

9.2.6.5.1.1. Considerar portas não escaneadas como fechadas;

9.2.6.5.1.2. Range de portas a serem escaneadas;

9.2.6.6. Enumerar Portas locais:

9.2.6.6.1. SSH (netstat);

9.2.6.6.2. WMI (netstat);

9.2.6.6.3. SNMP;

9.2.7. Da descoberta de serviços

9.2.7.1. Sondar todas as portas para encontrar serviços;

9.2.7.2. Procurar por serviços baseado em SSL/TLS;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

9.2.7.3. Enumerar todas as cifras SSL/TLS;

9.2.8. A solução deve realizar descoberta de ativo de forma passiva e adicionado automaticamente na console de gerenciamento;

9.2.9. A solução deve descobrir passivamente quando um *host* é adicionado na rede;

9.2.10. Da avaliação de vulnerabilidade

9.2.10.1. A solução deve ser capaz de realizar testes sem a necessidade de agentes instalados no dispositivo destino para detecção de vulnerabilidades;

9.2.10.2. A solução deve detectar e classificar através de severidades, riscos e vulnerabilidades;

9.2.10.3. A solução deve também fornecer informações detalhadas sobre a natureza da vulnerabilidade, evidências da existência da vulnerabilidade e recomendações para mitigá-los;

9.2.10.4. A solução deve incluir uma saída detalhada das vulnerabilidades descobertas como versões de DLL esperadas e encontradas;

9.2.10.5. A solução deve ser compatível com CVE e fornecer pelo menos 10 anos de cobertura CVE;

9.2.10.6. A solução deve identificar vulnerabilidades específicas para o *Active Directory* com os seguintes padrões de verificação;

9.2.10.6.1. Contas administrativas vulneráveis a *Kerberoasting Attack*;

9.2.10.6.2. Utilização de criptografia vulnerável com autenticação *Kerberos*;

9.2.10.6.3. Contas com pré-autenticação do *Kerberos* desabilitada;

9.2.10.6.4. Verificação de usuários com a opção de nunca expirar a senha com a opção habilitada;

9.2.10.6.5. Verificar validação de fragilidades do tipo “Unconstrained Delegation”;

9.2.10.6.6. Verificação de “Pre-Windows 2000 Compatible Access”;

9.2.10.6.7. Verificação de validade de chaves mestras “Kerberos KRBTGT”;

9.2.10.6.8. Verificação de “SID History Injection”;

9.2.10.6.9. Verificação de “Printer Bug Exploit”;

9.2.10.6.10. Verificação de “Primary Group ID”;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 9.2.10.6.11. Verificação de usuários com *Passwords* em branco;
- 9.2.10.7. A solução deve suportar o uso de SMB e WMI para verificação de sistemas Microsoft Windows;
- 9.2.10.8. A solução deve ser capaz de iniciar automaticamente serviços de registro remoto em sistemas Windows ao executar uma varredura credenciada;
- 9.2.10.9. A solução deve ser capaz de parar automaticamente o serviço de registro remoto em sistemas Windows novamente assim que a varredura estiver completa;
- 9.2.11. O Scanner deve oferecer suporte a Shell seguro (SSH) com a capacidade de escalar privilégios para varredura de vulnerabilidades e auditorias de configuração em sistemas Unix;
- 9.2.11.1. A solução deve suportar o uso do Netstat (Linux) e WMI (Windows) para uma enumeração rápida e precisa de portas em um sistema quando as credenciais são fornecidas;
- 9.2.11.2. A solução deve possibilitar a verificação remota de portas, além da enumeração local de portas, para ajudar a determinar se algum mecanismo de controle de acesso está sendo utilizado;
- 9.2.11.3. A solução deve fornecer auditoria de Patch (MS Bulletins) para as principais versões de Windows;
- 9.2.11.4. A solução deve fornecer auditoria de Patch para todos os principais sistemas operacionais Unix incluindo Mac OS, Linux, Solaris e IBM AIX;
- 9.2.11.5. A solução deve fornecer varredura para aplicativos comerciais diversos e proprietários, incluindo, mas não limitando-se a: Java, Adobe, Oracle, Apple, Microsoft, Check Point, Palo Alto Networks, Cisco, Fortinet, Fireeye, McAfee, etc;
- 9.2.11.6. A solução deve incluir classificação de severidades de acordo com o padrão Sistema Comum de Pontuação de Vulnerabilidade Versão (CVSS2 e CSVSS 3);
- 9.2.11.7. A solução deve fornecer informações acerca da disponibilidade de códigos de exploração das vulnerabilidades encontradas em Frameworks de exploração para as plataformas mais populares: Core, Metasploit e Canvas;
- 9.2.11.8. A solução deve informar se a vulnerabilidade pode e está sendo ativamente explorada por código malicioso (Malware);
- 9.2.11.9. A solução deve possuir importação de arquivos .YARA;
- 9.2.11.10. Deve ser capaz de identificar e classificar vulnerabilidades de máquinas virtuais em nuvem pública em infraestruturas como serviço nas plataformas AWS, Microsoft Azure e Google Cloud;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

9.2.12. Da auditoria de Configuração

9.2.12.1. A solução deve ser capaz de realizar auditoria de conformidade sem a necessidade de agente instalado no dispositivo de destino;

9.2.12.2. A solução deve fornecer *Benchmarks* de auditoria de segurança e configuração para conformidade regulatória e outros padrões de práticas recomendadas pela área ou fabricantes;

9.2.12.3. A solução deve realizar verificações de auditoria contendo as de segurança, com indicação de sucesso ou falha, baseado nos principais *Frameworks* reconhecidos pela indústria, pelo menos os seguintes:

9.2.12.3.1. *Center for Internet Security Benchmarks* (CIS);

9.2.12.3.2. *Defense Information Systems Agency* (DISA) STIGs;

9.2.12.3.3. *Health Insurance Portability and Accountability Act* (HIPAA);

9.2.12.3.4. *Payment Card Industry Data Security Standards* (PCI DSS);

9.2.12.4. A solução deve fornecer auditoria de programas antivírus para determinação de presença e *Status* de inicialização para no mínimo os seguintes produtos: TrendMicro Office Scan, McAfee VirusScan, Microsoft Endpoint Protection e Kaspersky;

9.2.12.5. A solução deve fornecer auditorias de configuração com base *Benchmarks* em CIS (*Center for Internet Security*) L1 e L2, para ambos os sistemas operacionais Microsoft Windows e Linux;

9.2.12.6. A solução deve permitir auditoria de conformidade em servidores Windows, Linux, Bancos de Dados SQL Server, a fim de determinar se estão configurados de acordo com os principais Framework de segurança como, por exemplo, CIS e DISA;

9.2.12.7. A solução deve oferecer validação e suporte a SCAP (*Security Content Automation Protocol*);

9.2.13. Análise dinâmica de vulnerabilidades para aplicações Web

9.2.13.1. A solução deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web como parte dos ativos a serem inspecionados;

9.2.13.2. A solução deve ser capaz de executar varreduras em sistemas web através de seus endereços IP ou FQDN (DNS);

9.2.13.3. A solução deve avaliar no mínimo os padrões de segurança OWASP Top 10 e PCI (*Payment Card Industry Data Security Standard*);

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 9.2.13.4. A solução deve suportar as diretivas PCI ASV 5.5 para definição de escopo de análise da aplicação;
- 9.2.13.5. A solução deve suportar as diretivas PCI ASV 6.1 para definição de balanceadores de carga das aplicações bem como suas configurações para inclusão no relatório de resultados;
- 9.2.13.6. A solução deve possuir *Templates* prontos de varreduras entre simples e extensos;
- 9.2.13.7. Para varreduras extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos:
- 9.2.13.7.1. *Cookies, Headers, Formulários e Links*;
 - 9.2.13.7.2. Nomes e valores de parâmetros da aplicação;
 - 9.2.13.7.3. Elementos JSON e XML;
 - 9.2.13.7.4. Elementos DOM;
- 9.2.13.8. A solução deve permitir somente a execução da função *Crawler*, que consiste na navegação para descoberta das URLs existentes na aplicação;
- 9.2.13.9. A solução deve ser capaz de utilizar *Scripts* customizados de *Crawl* com parâmetros definidos pelo usuário;
- 9.2.13.10. A solução deve excluir determinadas URLs da varredura através de expressões regulares;
- 9.2.13.11. A solução deve excluir determinados tipos de arquivos através de suas extensões;
- 9.2.13.12. A solução deve instituir no mínimo os seguintes limites:
- 9.2.13.12.1. Número máximo de URLs para *Crawl* e navegação;
 - 9.2.13.12.2. Número máximo de diretórios para varreduras;
 - 9.2.13.12.3. Número máximo de elementos DOM;
 - 9.2.13.12.4. Tamanho máximo de respostas;
 - 9.2.13.12.5. Limite de requisições de redirecionamentos;
 - 9.2.13.12.6. Tempo máximo para a varredura;
 - 9.2.13.12.7. Número máximo de conexões HTTP ao servidor hospedando a aplicação Web;
 - 9.2.13.12.8. Número máximo de requisições HTTP por segundo.
- 9.2.13.13. A solução deve detectar congestionamento de rede e limitar os seguintes aspectos da

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

varredura:

- 9.2.13.13.1. Limite em segundos para *Timeout* de requisições de rede;
- 9.2.13.13.2. Número máximo de *Timeouts* antes que a varredura seja abortada;
- 9.2.13.14. A solução deve agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;
- 9.2.13.15. A solução deve enviar notificações através de no mínimo *E-mail* e SMS;
- 9.2.13.16. A solução deve possuir a flexibilidade de selecionar quais testes serão realizados de forma granular, através da seleção de testes, *Plug-ins* ou ataques;
- 9.2.13.17. A solução deve avaliar sistemas web utilizando protocolos HTTP e HTTPS;
- 9.2.13.18. A solução deve possibilitar a definição de atributos no cabeçalho (*HEADER*) da requisição HTTP de forma personalizado a ser enviada durante os testes;
- 9.2.13.19. A solução deve ser compatível com avaliação de *Web Services* REST e SOAP;
- 9.2.13.20. Deverá suportar no mínimo os seguintes esquemas de autenticação:
 - 9.2.13.20.1. Autenticação básica (*Digest*);
 - 9.2.13.20.2. NTLM;
 - 9.2.13.20.3. *Form de Login*;
 - 9.2.13.20.4. Autenticação de *Cookies*;
 - 9.2.13.20.5. Autenticação através de *Selenium*;
 - 9.2.13.20.6. Autenticação através de *Bearer*;
- 9.2.13.21. A solução deve importar *Scripts* de autenticação *Selenium* previamente configurados pelo usuário;
- 9.2.13.22. A solução deve customizar parâmetros *Selenium* como *Delay* de exibição da página, *Delay* de execução de comandos e *Delay* de comandos para recepção de novos comandos;
- 9.2.13.23. A solução deve exibir os resultados das varreduras em tendência temporal para acompanhamento de correções e introdução de novas vulnerabilidades;
- 9.2.13.24. A solução deve exibir os resultados agregados de acordo com as categorias do OWASP Top 10 (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project);

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

9.2.13.25. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;

9.2.13.26. Para cada vulnerabilidade encontrada, deve ser exibido evidências da mesma em seus detalhes;

9.2.13.27. Para vulnerabilidades de injeção de código (SQL, XSS, XSRF etc.), deve evidenciar nos detalhes do evento encontrado:

9.2.13.27.1. *Payload* injetado;

9.2.13.27.2. Evidência em forma de resposta da aplicação;

9.2.13.27.3. Detalhes da requisição HTTP;

9.2.13.27.4. Detalhes da resposta HTTP;

9.2.13.28. Os detalhes das vulnerabilidades devem conter descrição da falha e referências didáticas para a revisão dos analistas;

9.2.13.29. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação das mesmas;

9.2.13.30. A solução deve possuir suporte a varreduras de componentes para no mínimo:

9.2.13.30.1. Wordpress, Blog Designer Plugin for Wordpress, Event Calendar Plugin for Wordpress, Convert Plus Plugin for Wordpress, AngularJS, Apache, Apache Tomcat, Apache Tomcat JK connecto, Apache Spark e Apache Struts, Atlassian Confluence, Atlassian Crowd e Atlassian Jira, Backbone.js, ASP.NET, Bootstrap, Drupal, Joomla!, jQuery, Lighttpd, Magento, Modernizr, Nginx, PHP, AJAX, Sitefinity, Telerik, ThinkPHP, Webmin e YUI;

9.2.14. Solução de análise de infraestrutura sobre código em ambiente de Imagens em Contêiner, DevOps e GitOps.

9.2.14.1. A solução deve detectar e configurações incorretas da infraestrutura de nuvem em fases de design, construção e tempo de execução do seu ciclo de vida de desenvolvimento de software;

9.2.14.2. A solução deve prevenir problemas de segurança identifique e remova falhas na nuvem durante desenvolvimento antes de chegarem à produção;

9.2.14.3. A solução deve ser possível avaliar modelos de infraestrutura como código (IaC), com integrações nativas em:

9.2.14.3.1.1. Terraform;

9.2.14.3.1.2. AWS CloudFormation;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

9.2.14.3.1.3. Azure Resource Manager;

9.2.14.3.1.4. Kubernetes;

9.2.14.4. A solução deve prevenir o desvio de postura na nuvem identifique discrepâncias entre o IaC e sua nuvem em execução ambiente;

9.2.14.5. A solução deve fornecer sugestões de correção automaticamente por meio de pull ou mesclagem;

9.2.14.6. A solução deve contextualizar riscos compreender as vulnerabilidades de aplicativos no contexto de suas configurações de infraestrutura para obter uma imagem real do risco que eles presente;

9.2.14.7. A solução deve prover integração no mínimo com as seguintes plataformas abaixo:

9.2.14.7.1.1. Jira;

9.2.14.7.1.2. Slack;

9.2.14.7.1.3. AWS SNS;

9.2.14.7.1.4. Jenkins;

9.2.14.7.1.5. Terraform Cloud;

9.2.14.7.1.6. CircleCI;

9.2.14.7.1.7. Splunk;

9.2.14.7.1.8. AWS CloudTrail;

9.2.14.8. A solução deve possuir integração com no mínimo os seguintes Repositórios:

9.2.14.8.1.1. Bitbucket;

9.2.14.8.1.2. GitHub;

9.2.14.8.1.3. GitLab;

9.2.14.8.1.4. Azure DevOps;

9.2.14.9. A solução deve possuir funcionalidade de monitoramento dos repositórios sempre que houver alteração de código uma verificação automática via IaC deve apresentar a diferença;

9.2.14.10. A solução deve possuir políticas de análise em ambiente de nuvem para no mínimo as seguintes plataformas:

9.2.14.10.1.1. AWS;

9.2.14.10.1.2. Azure;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 9.2.14.10.1.3. GCP;
- 9.2.14.10.1.4. Kubernetes;

9.2.15. A solução deve possuir análise por benchmarks e compliance para os seguintes padrões em formato de Dashboard:

- 9.2.15.1. CIS;
- 9.2.15.2. NIST;
- 9.2.15.3. ISO-27001;
- 9.2.15.4. HIPAA;
- 9.2.15.5. PCI-DSS;
- 9.2.15.6. CCM;
- 9.2.15.7. GDPR;
- 9.2.15.8. A solução deve analisar, testar e reportar falhas de segurança em aplicações em Containers Docker como parte dos ativos a serem inspecionados;
- 9.2.15.9. A solução deve ser capaz de analisar imagens preparadas pelos desenvolvedores na esteira DevOps em busca de imagens com vulnerabilidades identificadas e malware residente no sistema de arquivos;
- 9.2.15.10. A solução deve integrar a esteira DevOps através de API, invocando o envio da imagem para análise em repositório próprio da solução ou utilizando scanner implementado em infraestrutura proprietária do órgão com a finalidade de evitar o envio de imagens e propriedade intelectual da contratante;
- 9.2.15.11. A documentação de API da solução deverá ter acesso público através de website ou documentação do próprio fabricante;
- 9.2.15.12. A console de administração deverá possuir controle de acesso no mínimo permitindo usuários com capacidade de somente visualizar as informações, e usuários com capacidade para efetuar análise das imagens;
- 9.2.15.13. A solução deve inventariar o sistema operacional de cada imagem analisada e suas vulnerabilidades encontradas;
- 9.2.15.14. A solução deve identificar containers que não foram analisados antes de sua implementação em produção;
- 9.2.15.15. A solução deve analisar as camadas (layers) de um container;
- 9.2.15.16. A solução deve identificar containers que tiveram mudanças de arquivos entre a análise

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

e a sua implementação em produção;

9.2.15.17. A solução deve informar os CVEs para cada vulnerabilidade encontrada nos pacotes e bibliotecas residentes na imagem;

9.2.15.18. A solução deve ter a capacidade de testar automaticamente todas as imagens armazenadas, ou previamente testadas, sempre que uma nova vulnerabilidade for publicada e atualizada no banco de dados de vulnerabilidade da solução, sem qualquer tipo intervenção manual;

9.2.15.19. A solução deve inventariar os pacotes e bibliotecas e suas respectivas versões e listar as mesmas dentro do relatório de resultados de análise de cada imagem;

9.2.15.20. A solução deve possuir conectores e permitir importação de imagens dos seguintes repositórios:

- 9.2.15.20.1.1. - Docker;
- 9.2.15.20.1.2. - Docker EE;
- 9.2.15.20.1.3. - AWS ECR;
- 9.2.15.20.1.4. - JFrog Artifactory;

9.2.15.21. A solução deve possuir integração com Microsoft Azure Container, Vmware Harbor e Sonatype Nexus para importar e analisar imagens;

9.2.15.22. A solução deve fornecer scanner em formato Docker para implementação local e análise de imagens sem a necessidade de envio destas para repositório remoto, fora do ambiente da contratante;

9.2.15.23. A solução ser capaz de configurar políticas usando como condições: CVSS Score, CVEs específicos e Malware identificado;

9.2.15.24. A solução deve permitir a criação de políticas específicas por repositório;

9.2.15.25. A solução deve prover integração com as seguintes plataformas de integração contínua: Bamboo, CircleCI, Codeship, Distelli, Drone.io, Jenkins, Shippable, Solano Labs, Travis CI, Wrecker e Kubernetes;

9.2.16. Da Análise em ambiente Microsoft *Active Directory*

9.2.16.1. A solução deve identificar fraquezas ocultas em configurações dedicadas ao *Active Directory*;

9.2.16.2. A solução deve possuir ações preventivas de *Hardening* para o *Active Directory*;

9.2.16.3. A solução deve identificar ataque específicos para a estrutura do *Active Directory*;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 9.2.16.4. A solução deve possuir funcionalidade para analisar em detalhes cada configuração incorreta que acarreta riscos de segurança – com uma linguagem simples, contextualizando tal risco para os times envolvidos;
- 9.2.16.5. A solução deve possuir recomendações de correção para cada configuração incorreta no *Active Directory*;
- 9.2.16.6. A solução deve avaliar relações de confiança perigosas entre florestas e domínios;
- 9.2.16.7. A solução deve capturar as mudanças que ocorrem no AD e demonstrar na console de administração;
- 9.2.16.8. A solução deve possuir *Dashboard* com os principais ataques e vulnerabilidades por domínio;
- 9.2.16.9. A solução deve permitir a correlação de mudanças no *Active Directory* e desvios de segurança;
- 9.2.16.10. A solução deve analisar em detalhes um ataque explorando as descrições através do *Framework* MITRE ATT&CK;
- 9.2.16.11. A solução deve prover interface web para gerenciamento de todas as funcionalidades;
- 9.2.16.12. A solução deve possuir capacidade nativa de criação de *Dashboards* customizados;
- 9.2.16.13. A solução deve suportar um modelo de controle de acesso baseado em funções (RBAC) flexível;
- 9.2.16.14. A solução deve realizar alterações no *Active Directory*, seus objetos e atributos;
- 9.2.16.15. A solução deve armazenar ou sincronizar nenhuma credencial de objetos do *Active Directory*;
- 9.2.16.16. A solução deve suportar ambientes com múltiplas florestas e domínios;
- 9.2.16.17. A solução deve suportar monitoramento contínuo de ambientes com *Active Directory* com o nível funcional de floresta e domínio a partir do 2003;
- 9.2.16.18. A solução deve suportar e reter os eventos coletados por no mínimo um ano;
- 9.2.16.19. A solução deve descobrir e mapear a superfície de ataque do *Active Directory* e seus domínios monitorados com os seguintes padrões:
- 9.2.16.19.1.1. Não depender de agentes ou sensores para coleta de informações do AD;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

9.2.16.19.1.2. A solução deve seguir as boas práticas de *menor privilégio*, a conta de serviço utilizada para conexão com o *Active Directory*, sendo o menor nível de acesso esperado para a conta de serviço como parte do grupo *Domain User*;

9.2.16.19.1.3. Interface web que consolida e apresenta de maneira unificada os domínios monitorados e as possíveis relações de confiança estabelecidas entre eles;

9.2.16.20. A solução deve analisar continuamente a postura de segurança do AD, minimamente avaliando:

9.2.16.20.1. Validação de GPOs desvinculadas, desabilitadas ou órfãs;

9.2.16.20.2. Validação de contas desativadas em grupos privilegiados;

9.2.16.20.3. Domínio usando uma configuração perigosa de compatibilidade com versões anteriores por meio de alterações no atributo *dSHeuristics*;

9.2.16.20.4. Validação de atributos relacionados a roaming de credenciais vulneráveis (*ms-PKI-DPAPIMasterKeys*) gerenciados por um usuário sem privilégios;

9.2.16.20.5. Validação de domínio sem GPOs de proteção de computador, desativando protocolos vulneráveis antigos, como *NTLMv1*;

9.2.16.20.6. Validação de contas com senhas que nunca expiram;

9.2.16.20.7. Validação de senhas reversíveis em GPOs;

9.2.16.20.8. Validação de uso de senhas reversíveis em contas de usuário;

9.2.16.20.9. Validação de utilização de protocolo criptográfico fraco (Ex. DES) em contas de usuário;

9.2.16.20.10. Validação de uso do LAPS (Solução de senha de administrador local) para gerenciar senhas de contas locais com privilégios;

9.2.16.20.11. Validação se o domínio possui um nível funcional desatualizado;

9.2.16.20.12. Validação de contas de usuário utilizando senha antiga;

9.2.16.20.13. Validação se o atributo *AdminCount* está definido em usuários padrão;

9.2.16.20.14. Validação do uso recente da conta de administrador padrão;

9.2.16.20.15. Validação de usuários com permissão para ingressar computadores no domínio;

9.2.16.20.16. Validação de contas dormentes;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 9.2.16.20.17. Validação de computadores executando um sistema operacional obsoleto;
- 9.2.16.20.18. Validação de restrições de *Logon* para usuários privilegiados em ambiente com múltiplos *Tiers* (1, 2 e 3) de segregação de ativos;
- 9.2.16.20.19. Validação de direitos perigosos configurados no *Schema* do AD;
- 9.2.16.20.20. Validação de relação de confiança perigosa com outras *Florestas* e *Domínios*;
- 9.2.16.20.21. Validação de contas que possuem um atributo perigoso de histórico SID (*SID History*);
- 9.2.16.20.22. Validação de contas utilizando controle de acesso compatível com versões anteriores ao Windows 2000;
- 9.2.16.20.23. Validação da última alteração de senha do KDC;
- 9.2.16.20.24. Validação da última alteração da senha da conta SSO do *Azure AD*;
- 9.2.16.20.25. Validação de contas que podem ter senha em branco/vazia;
- 9.2.16.20.26. Validação de utilização do grupo nativo *Protected Users*;
- 9.2.16.20.27. Validação de privilégios sensíveis (Ex. *Debug a program*, *Replace a process level token*, etc.) perigosos atribuídos aos usuários;
- 9.2.16.20.28. Validação de possível senha em *Clear-Text*;
- 9.2.16.20.29. Validação de sanidade das GPOs e componentes CSEs (*Client-Side Extension*);
- 9.2.16.20.30. Validação de uso de algoritmos de criptografia fracos na PKI do *Active Directory*;
- 9.2.16.20.31. Validação de contas de serviço com SPN (*Service Principal Name*) que fazem parte de grupos privilegiados;
- 9.2.16.20.32. Validação de contas anormais nos grupos administrativos padrão do AD;
- 9.2.16.20.33. Validação de consistência no *container adminSDHolder*;
- 9.2.16.20.34. Validação de delegação *Kerberos* perigosa;
- 9.2.16.20.35. Validação em permissões de objetos raiz que permitem ataques do tipo DCSync;
- 9.2.16.20.36. Validação de políticas de senha fracas aplicadas aos usuários;
- 9.2.16.20.37. Validação das permissões relacionadas às contas do *Azure AD Connect*;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 9.2.16.20.38. Validação do ID do grupo primário do usuário (*Primary Group ID*);
- 9.2.16.20.39. Validação de permissões em GPOs sensíveis associadas aos *Containers Configuration*, *Sites*, *Root Partition* e *OUs* sensíveis como *Domain Controllers*;
- 9.2.16.20.40. Controladores de domínio gerenciados por usuários ilegítimos;
- 9.2.16.20.41. Validação de certificado mapeado através de atributo *altSecurityIdentities* em contas privilegiadas;
- 9.2.16.20.42. Validação de uso de protocolo *Netlogon* inseguro (*ZeroLogon/CVE-2020-1472*);
- 9.2.16.21. A solução deve identificar vulnerabilidades e configurações incorretas do AD à medida que são introduzidas sendo:
- 9.2.16.21.1. Identificar todas as vulnerabilidades e configurações incorretas no AD;
 - 9.2.16.21.2. Monitorar relações de confiança perigosas em toda a estrutura AD;
 - 9.2.16.21.3. Apresentar ameaças e alterações sem a necessidade de *Scans* estáticos e programados no *Active Directory* e sua infraestrutura;
 - 9.2.16.21.4. Apresentar as ameaças e alterações em tempo real ou em menos de cinco minutos;
- 9.2.16.22. Detecção e resposta a ataques:
- 9.2.16.22.1. Monitorar continuamente os indicadores de possíveis ataque como *DCSync*, *DCShadow*, *Password Spraying*, *Password Guessing/Brute Force*, *Lsaas Injecton* nos controladores de domínio, *Golden Ticket*, *NTLM Relay*, entre outros;
 - 9.2.16.22.2. Detecção de ataques ao AD em tempo real ou em menos de um minuto;
 - 9.2.16.22.3. Análise detalhada do ataque, apresentando ativo de origem, vetor de ataque, controlador de domínio afetado, técnica aplicada;
 - 9.2.16.22.4. Apresentação de ataques em uma linha do tempo;
 - 9.2.16.22.5. Investigar ameaças, reproduzir ataques e procurar por *Backdoors*;
 - 9.2.16.22.6. Permitir busca ágil de eventos específicos na base da solução através de queries customizadas;
- 9.2.16.23. A solução deve ser capaz de enviar alertas por e-mail;
- 9.2.16.24. A solução nativamente deve ser capaz de se integrar com SIEM através de protocolo

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

SYSLOG;

- 9.2.16.25. A solução deve ser capaz de filtrar e enriquecer os eventos que serão enviados para o SIEM;
- 9.2.16.26. A solução deve produzir regras YARA na detecção de ataques (Ex. DCSync, Golden Ticket) identificados pela ferramenta;
- 9.2.16.27. A solução deve possuir conjunto de APIs REST, todas as chamadas disponíveis devem estar contidas na documentação;
- 9.2.16.28. A solução deve permitir a criação de listas de exclusões, suportando minimamente Exclusão por domínios do AD monitorados e por itens analisados;
- 9.2.16.29. A solução deve ser licenciada pelo número de usuários habilitados.

9.3. PROCESSO DE EXECUÇÃO DO SERVIÇO PARA GESTÃO DE VULNERABILIDADES

- 9.3.1. A fim de balizar todo o processo de gestão de vulnerabilidade da CONTRATANTE, e influenciado pelos principais *Frameworks* de boas práticas de serviços de segurança da informação, foi arquitetado o processo que será descrito nos parágrafos que seguem, o qual obrigatoriamente a CONTRATADA deve seguir *ipsis litteris*.
- 9.3.2. A CONTRATANTE deverá apresentar uma lista de ativos e recursos que deverão fazer parte do processo de gestão de vulnerabilidade. Tal lista poderá ser revisada e atualizada durante todo o período de vigência de contrato e deverá conter as seguintes informações mínimas, a saber:
- a) Nome do ativo e/ou serviço;
 - b) Grupo de serviço;
 - c) IP;
 - d) Janela de análise (Horário permitido para análise);
 - e) Prioridade.
- 9.3.3. A CONTRATADA deverá realizar de forma continuada uma avaliação prévia no ambiente computacional da CONTRATANTE a fim de consultivamente sugerir e complementar a lista de ativos e recursos que deverão fazer parte do processo de gestão de vulnerabilidade.
- 9.3.4. De acordo com as variáveis e critérios estabelecidos no catálogo de serviço e na lista de ativos e recursos da CONTRATANTE, a CONTRATADA deverá realizar checagens (*Scans*) e varreduras, buscando encontrar vulnerabilidades de segurança no ambiente da CONTRATANTE, utilizando as ferramentas e soluções definidas no presente termo de referência.
- 9.3.5. Após o término das rotinas de checagens (*Scans*) e varreduras no ambiente, deverá a CONTRATADA realizar uma análise de falso positivo das vulnerabilidades descobertas, isso

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

quer dizer, que devem ser informadas à CONTRATANTE apenas vulnerabilidades que existam de fato em seu ambiente.

- 9.3.6. Após análise de falso positivo, a CONTRATADA deverá informar ao CONTRATANTE as vulnerabilidades encontradas, obedecendo os critérios e requisitos estabelecidos no presente termo de referência.
- 9.3.7. Uma vez autorizada a mudança para correção de uma determinada vulnerabilidade, caberá a CONTRATADA sugerir as correções de vulnerabilidades encontradas no ambiente listado no tópico AMBIENTE TECNOLÓGICO DA CONTRATANTE (Hardware e Software), obrigatoriamente obedecendo as definições proposta pelo comitê de mudança da CONTRATANTE.
- 9.3.8. Para as vulnerabilidades encontradas no ambiente que ainda não tiverem soluções conhecidas, caberá à CONTRATADA apresentar medidas de contorno, que para aplicá-las ao ambiente, deverá obedecer ao ciclo de mudança estabelecido nos parágrafos anteriores.
- 9.3.9. Como último passo, a CONTRATADA deverá atualizar todos os controles e indicadores estabelecidos no presente termo de referência.
- 9.3.10. O processo descrito é o mínimo esperado a ser seguido e executado pela CONTRATADA. Todavia, como o objeto do presente termo de referência se trata de um serviço continuado, logo, se espera da CONTRATADA a apresentação de melhoria contínua deste, o qual pode ser alterado desde que aprovado pela CONTRATANTE.
- 9.3.11. O ciclo de vida do processo de gestão de vulnerabilidade deve ser executado de forma recorrente. A recorrência é definida em execuções de *Scans* quinzenais e apresentação dos resultados de forma mensal.

9.4. GRUPO TÉCNICO PARA EXECUÇÃO DO SERVIÇO

- 9.4.1. Através do seu Centro de Operações de Segurança definidos e especificados neste certame, a CONTRATADA deverá manter uma torre de operação denominada GRUPO DE ATAQUE CIBERNÉTICO CONTROLADO (Red Team), com objetivo e foco de trabalhar no processo de gestão de vulnerabilidade.
- 9.4.2. Estes profissionais deverão ser exclusivos para trabalhar no GRUPO DE ATAQUE CIBERNÉTICO (Red Team), não podendo os profissionais pertencentes a este grupo serem compartilhados e/ou atuarem com os demais serviços descritos no objeto do presente termo de referência.
- 9.4.3. Todos os profissionais que integram o grupo de ataque cibernético controlado devem obrigatoriamente compor o quadro permanente de colaboradores da CONTRATADA em regime de trabalho CLT (Consolidação das Leis do Trabalho) ou contrato de prestação de serviços firmados diretamente entre esses profissionais e a CONTRATADA, não havendo a possibilidade de terceirização ou subcontratação de tal serviço.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 9.4.4. Deverá ser de responsabilidade da CONTRATADA dimensionar o número adequado de profissionais para entrega de tal serviço sem que haja impacto no acordo de nível de serviço estabelecido no item Gestão de Vulnerabilidade do presente termo de referência.
- 9.4.5. A fim de garantir que os profissionais envolvidos tenham conhecimento e habilidade para executar o processo de gestão de vulnerabilidades no ambiente da CONTRATANTE, a CONTRATADA obrigatoriamente deverá compor o GRUPO DE ATAQUE CIBERNÉTICO CONTROLADO (*Red Team*) com ao menos 1 (um) perfil de cada que segue descrito abaixo:

Certificações	Descrição
- Linux LPIC 1, Linux LPIC 2 ou Linux LPIC 3 - CompTIA Security+ ou Certified Ethical Hacker	Diploma, devidamente registrado de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.

Tabela 4 - Certificações Grupo de Ataque Cibernético Controlado

- 9.4.6. Não existe restrição ou limite para acúmulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos no GRUPO DE ATAQUE CIBERNÉTICO CONTROLADO (*Red Team*), porém conforme já fora mencionado no presente termo de referência, este(s) deve(m) compor único e exclusivamente o time denominado GRUPO DE ATAQUE CIBERNÉTICO CONTROLADO (*Red Team*).
- 9.4.7. No momento da assinatura do contrato será exigido da CONTRATADA as seguintes documentações do(s) profissionais que participarão do GRUPO DE ATAQUE CIBERNÉTICO CONTROLADO (*Red Team*), os quais devem comprovar as exigências e obrigações descritas no presente termo de referência: contrato de prestação de serviços ou carteira de trabalho devidamente assinada pela CONTRATADA e as devidas certificações técnicas para comprovação do conhecimento.

9.5. ENTREGAS A SEREM REALIZADAS

- 9.5.1. Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, a CONTRATANTE definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue de forma *On Line* e em tempo de execução, através do portal de segurança descrito no tópico de condições gerais para prestação do serviço deste

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

termo de referência, a saber:

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Quantitativo de vulnerabilidades	Soma de vulnerabilidades	Vulnerabilidades	Vulnerabilidades	Número total de vulnerabilidades
Quantitativo de vulnerabilidades de severidade 5 por área responsável	Soma de vulnerabilidades de severidade 5 por área responsável	Vulnerabilidades de severidade 5	Vulnerabilidades	Número total de vulnerabilidades de severidade 5 por área responsável
Quantitativo de vulnerabilidades de severidade 4 por área responsável	Soma de vulnerabilidades de severidade 4 por área responsável	Vulnerabilidades de severidade 4	Vulnerabilidades	Número total de vulnerabilidades de severidade 4 por área responsável
Quantitativo de novas vulnerabilidades de severidades 4 e 5 por área responsável	Soma de novas vulnerabilidades de severidades 4 e 5 por área responsável	Vulnerabilidades de severidades 4 e 5	Vulnerabilidades	Número total de novas vulnerabilidades de severidades 4 e 5 por área responsável
Quantitativo de vulnerabilidades corrigidas de severidades 4 e 5 por área responsável	Soma de vulnerabilidades corrigidas de severidades 4 e 5 por área responsável	Vulnerabilidades corrigidas de severidades 4 e 5	Vulnerabilidades	Número total de vulnerabilidades corrigidas de severidades 4 e 5 por área responsável
Quantitativo de vulnerabilidades em Aplicações WEB	Soma de vulnerabilidades em Aplicações WEB	Vulnerabilidades em Aplicações WEB	Vulnerabilidades	Número total de vulnerabilidades em Aplicações WEB
Quantitativo de vulnerabilidades em Aplicações WEB de severidade 5	Soma de vulnerabilidades em Aplicações WEB de severidade 5	Vulnerabilidades em Aplicações WEB de severidade 5	Vulnerabilidades	Número total de vulnerabilidades em Aplicações WEB de severidade 5
Quantitativo de vulnerabilidades em Aplicações WEB de severidade 4	Soma de vulnerabilidades em Aplicações WEB de severidade 4	Vulnerabilidades em Aplicações WEB de severidade 4	Vulnerabilidades	Número total de vulnerabilidades em Aplicações WEB de severidade 4
Quantitativo de novas vulnerabilidades em Aplicações WEB de	Soma de novas vulnerabilidades em Aplicações WEB de	Vulnerabilidades em Aplicações WEB de	Vulnerabilidades	Número total de novas vulnerabilidades em aplicações WEB de severidades 4 e 5

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

WEB de severidades 4 e 5	severidades 4 e 5	severidades 4 e 5		
Quantitativo de vulnerabilidades corrigidas em Aplicações WEB de severidades 4 e 5	Soma de vulnerabilidades corrigidas em Aplicações WEB de severidades 4 e 5	Vulnerabilidades corrigidas em Aplicações WEB de severidades 4 e 5	Vulnerabilidades	Número total de vulnerabilidades corrigidas em Aplicações WEB de severidades 4 e 5
Quantitativo de certificados digitais expirados	Soma de certificados digitais expirados	Certificados digitais expirados	Certificados digitais	Número total de certificados digitais expirados
Quantitativo de certificados digitais a expirar em 3 meses	Soma de certificados digitais a expirar em 3 meses	Certificados digitais a expirar em 3 meses	Certificados digitais	Número total de certificados digitais a expirar em 3 meses
TOP 10 – Ativos mais vulneráveis	Soma de vulnerabilidades por ativo	Vulnerabilidades por ativo	Vulnerabilidades	TOP 10 do número de vulnerabilidades por ativo
TOP 10 – Vulnerabilidades mais comuns em ativos	Soma de vulnerabilidades	Vulnerabilidades	Vulnerabilidades	TOP 10 do número de vulnerabilidades
TOP 10 – Áreas responsáveis com maior número de vulnerabilidades	Soma de vulnerabilidades por área responsável	Vulnerabilidades por área responsável	Vulnerabilidades	TOP 10 do número de vulnerabilidades por área responsável
TOP 10 – Áreas responsáveis com maior número de vulnerabilidades de severidade 4 e 5	Soma de vulnerabilidades de severidade 4 e 5 por área responsável	Vulnerabilidades de severidade 4 e 5 por área responsável	Vulnerabilidades	TOP 10 do número de vulnerabilidades de severidade 4 e 5 por área responsável
TOP 10 – Áreas responsáveis com percentual de vulnerabilidades de severidade 4 e 5	Percentual de vulnerabilidades de severidade 4 e 5 por área responsável	Vulnerabilidades de severidade 4 e 5 por área responsável	Vulnerabilidades	TOP 10 do percentual de vulnerabilidades de severidade 4 e 5 por área responsável
TOP 10 – Aplicações WEB mais vulneráveis	Soma de vulnerabilidades	Vulnerabilidades em Aplicações WEB	Vulnerabilidades	TOP 10 do número total de

Rua Cláudio Manoel, 639 - Savassi – Belo Horizonte/MG – Cep: 30140-105
 Telefone: (31) 3269-8400 - www.crcmg.org.br

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

	em Aplicações WEB			vulnerabilidades em Aplicações WEB
TOP 10 – Aplicações WEB mais vulneráveis em comparação com OWASP	Soma de vulnerabilidades em Aplicações WEB em comparação com OWASP	Vulnerabilidades em Aplicações WEB	Vulnerabilidades	TOP 10 do número total de vulnerabilidades em Aplicações WEB em comparação com OWASP

Tabela 5 - Indicadores Estratégicos Gestão de Vulnerabilidade

10. MONITORAMENTO, DETECÇÃO E RESPOSTA A INCIDENTES PARA ENDPOINTS

- 10.1.1. A operação e gerenciamento de proteção avançada de *Endpoint* deverá seguir os preceitos técnicos definidos abaixo com o intuito da CONTRATADA ofertar plataforma de gestão avançada de segurança para *Endpoint*, agregando qualidade e mais proteção ao processo;
- 10.1.2. Cabe à CONTRATADA toda operação, dos níveis mais básicos (Nível 1) até o mais avançado (Nível 3).
- 10.1.3. Deverá ser criado usuário de leitura para equipe da CONTRATANTE, limitado à 4 profissionais de segurança da informação, para acompanhamento das ações na console de gerenciamento.
- 10.1.4. SOBRE A FERRAMENTA A SER UTILIZADA
 - 10.1.4.1. Realizar a pré-execução do agente para verificar o comportamento malicioso e detectar *Malware* desconhecido;
 - 10.1.4.2. O agente deve buscar algum sinal de *Malware* ativo e detectar *Malwares* desconhecidos;
 - 10.1.4.3. O agente deve ter a capacidade de submeter o arquivo desconhecido à nuvem de inteligência do fabricante para detectar a presença de ameaças;
 - 10.1.4.4. O agente deve realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes;
 - 10.1.4.5. A solução deve manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência;
 - 10.1.4.6. Deve realizar a verificação de todos os arquivos acessados em tempo real, mesmo durante o processo de *Boot*;
 - 10.1.4.7. Deve realizar a verificação de todos os arquivos no disco rígido em intervalos programados;
 - 10.1.4.8. Deve realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA);

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 10.1.4.9. Deve proteger os navegadores Internet Explorer, Firefox, Chrome, Opera, Safari e Microsoft Edge, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados;
- 10.1.4.10. Deve permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos;
- 10.1.4.11. É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, *Spyware*, *Trojans*, *Worms*, *Adware* e aplicativos potencialmente indesejados (PUAs);
- 10.1.4.12. Suportar equipamentos com arquitetura 32-bit e 64-bit que o cliente deve ter instalado nas estações de trabalho e deve ser compatível com os sistemas operacionais: Mac OS X 10.10, 10.11, 10.12, Microsoft Windows XP SP3, 7, e 10;
- 10.1.4.13. Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção;
- 10.1.4.14. Permitir a utilização de senha de proteção para permitir a reconfiguração local no cliente ou desinstalação dos componentes de proteção;
- 10.1.4.15. Funcionalidade de Firewall e Detecção e Proteção de Intrusão para estação com as funcionalidades:
- 10.1.4.16. Deve possuir atualização periódica de novas assinaturas de ataque;
- 10.1.4.17. Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (*Hash*) do arquivo;
- 10.1.4.18. Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas;
- 10.1.4.19. Possuir um sistema de prevenção de intrusão na estação (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados.
- 10.1.4.20. Deve aplicar uma análise adicional, inspecionando finalmente o comportamento de códigos durante a execução, para detectar comportamento suspeito de aplicações, tais como *Buffer Overflow*.
- 10.1.4.21. Deve possuir técnicas de proteção, que inclui:
- 10.1.4.22. Análise dinâmica de código - técnica para detectar *Malware* criptografado mais complexo;
- 10.1.4.23. Algoritmo correspondente padrão - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificados como um vírus;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

10.1.4.24. Possuir capacidade para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;

10.1.4.25. Possuir tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo. jpg.txt) ou a extensão não coincide com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt);

10.1.4.26. Verificação de ameaças web avançadas: bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise comportamental para identificar e parar o código malicioso de *Malware* avançado.

10.1.5. Funcionalidades de Antivírus e *Antispyware*

10.1.5.1. Proteção em tempo real contra vírus, *Trojans*, *Worms*, *Rootkits*, *Botnets*, *Spyware*, *Adwares* e outros tipos de códigos maliciosos.

10.1.5.2. Proteção *Anti-Malware* nativa da solução ou incorporada automaticamente por meio de *Plug-ins* sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante.

10.1.5.3. As configurações do *Anti-Spyware* deverão ser realizadas através da mesma console do antivírus;

10.1.5.4. Permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou *Malware*, permitir a inclusão de arquivos em listas de exclusão (*Whitelists*) para que não sejam verificados pelo produto;

10.1.5.5. Permitir a varredura das ameaças da maneira manual, agendada e em tempo real na máquina do usuário;

10.1.5.6. Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos, através do antivírus;

10.1.5.7. Capacidade de remoção automática total dos danos causados por *Spyware*, *Adwares* e *Worms*, como limpeza do registro e pontos de carregamento, com opção de finalizar o processo e terminar o serviço da ameaça no momento de detecção;

10.1.5.8. A remoção automática dos danos causados deve ser nativa do próprio antivírus; ou adicionada por plugin, desde que desenvolvido ou distribuído pelo fabricante;

10.1.5.9. Capacidade de bloquear origem de infecção através de compartilhamento de rede com opção de bloqueio da comunicação via rede;

10.1.5.10. Permitir o bloqueio da verificação de vírus em recursos mapeados da rede;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

10.1.5.11. Antivírus de Web (verificação de *Sites* e *Downloads* contra vírus);

10.1.6. Controle de Acesso a *Sites* por Categoria

10.1.6.1. Proteger a navegação na *Web*, mesmo aos usuários fora da rede, para todos os principais navegadores (IE, Firefox, Safari, Opera, Chrome e Microsoft Edge), fornecendo controle da *Internet* independentemente do *Browser* utilizado, como parte da solução de proteção a estações de trabalho, incluindo a análise do conteúdo baixado pelo navegador *Web*, de forma independente do navegador usado, ou seja, sem utilizar um *Plugin*, onde não é possível ser ignorada pelos usuários, protegendo os usuários de *Websites* infectados.

10.1.6.2. Funcionalidades específicas para prevenção contra a ação de *Ransomwares*, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos ou a capacidade de fazer *Backup* de arquivos antes de serem criptografados para posteriormente permitir sua restauração.

10.1.7. Funcionalidade de detecção Pró-Ativa de reconhecimento de novas ameaças.

10.1.7.1. Funcionalidade de detecção de ameaças via técnicas de *Deep Machine Learning*;

10.1.7.2. Funcionalidade de detecção de ameaças desconhecidas que estão em memória;

10.1.7.3. Capacidade de detecção, e bloqueio pró-ativo de *Keyloggers* e outros *Malwares* não conhecidos (ataques de dia zero) através da análise de comportamento de processos em memória (heurística);

10.1.7.4. Capacidade de detecção e bloqueio de *Trojans* e *Worms*, entre outros *Malwares*, por comportamento dos processos em memória;

10.1.7.5. Capacidade de analisar o comportamento de novos processos ao serem executados, em complemento à varredura agendada.

10.1.8. Funcionalidades de proteção contra *Ransomware*

10.1.8.1. Dispor de proteção contra *Ransomware* não baseada exclusivamente na detecção por assinaturas;

10.1.8.2. Dispor de remediação da ação de criptografia maliciosa dos *Ransomwares*;

10.1.8.3. A solução deve prevenir ameaças e interromper que eles sejam executados em dispositivos da rede, detectando e limpando os *Malwares*, além da realização de uma análise detalhada das alterações realizadas.

10.1.8.4. Possuir uma tecnologia *Anti-Exploit* baseada em comportamento, reconhecendo e bloqueando as mais comuns técnicas de *Malware*, protegendo os *Endpoints* de ameaças

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

desconhecidas e vulnerabilidades *Zero-Day*.

10.1.8.5. Deve ser realizada a detecção e o bloqueio de, pelo menos, as seguintes técnicas de exploit:

- a) DEP (Data Execution Prevention);
- b) Address Space Layout Randomization (ASLR);
- c) Bottom Up ASLR;
- d) Null Page;
- e) Anti-HeapSpraying;
- f) Dynamic Heap Spray;
- g) Import Address Table Filtering (IAF);
- h) VTable Hijacking;
- i) Stack Pivot and Stack Exec;
- j) SEHOP;
- k) Stack-based ROP (Return-Oriented Programming);
- l) Control-Flow Integrity (CFI);
- m) Syscall;
- n) WOW64;
- o) Load Library;
- p) Shellcode;
- q) VBScript God Mode;
- r) Application Lockdown;
- s) Process Protection;
- t) Network Lockdown;
- u) Remote reflective DLL injection;

10.1.8.6. *Local Privilege Escalation* – LPE.

10.1.8.7. A solução deve trabalhar silenciosamente na máquina do usuário e deve detectar a criptografia maliciosa de dados (*Ransomware*), realizando a sua interrupção. No caso de arquivos serem criptografados a solução deve realizar o retorno destes arquivos ao seu estado normal. Deste modo a solução deve fazer a limpeza e remoção completa do *Ransomware* na máquina do usuário.

10.1.8.8. Deve fornecer também uma análise detalhada das modificações realizadas pelo *Ransomware*, realizando a correlação dos dados em tempo real, indicando todas as

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

modificações feitas em registros, chaves, arquivos alvos, conexões de redes e demais componentes contaminados.

- 10.1.8.9. A console de monitoração e configuração deve ser feita através de uma central única, baseada em *Web* e em nuvem ou *Appliance* físico, que deve conter todas a ferramentas para a monitoração e controle da proteção dos dispositivos para a solução de *Anti-Exploit* e *Anti-Ransomware*.
- 10.1.8.10. A console deve apresentar painel com o resumo detalhado de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional, bem como todas as identificações para o mapeamento instantâneo dos efeitos causados pelo *Ransomware* nas estações de trabalho.
- 10.1.8.11. A solução deve implementar técnicas de EDR (*Endpoint Detection and Response*), possibilitando detecção e investigação nos *Endpoints* com atividades suspeitas;
- 10.1.8.12. Em caso de incidente a solução deve mostrar a trilha da infecção de forma visual, mostrando o início, todas as interações do *Malware* e o ponto final de bloqueio.
- 10.1.8.13. Após a análise da nuvem de inteligência do fabricante a solução deve apresentar um relatório sobre a ameaça contendo no mínimo:
- 10.1.8.14. Detalhes do Processo, como nome, *Hash*, hora e data da detecção e remediação;
- 10.1.8.15. Resultado da análise do arquivo suspeito pela funcionalidade de *Machinne Learning* ou *Deep Learning*;
- 10.1.8.16. Propriedades gerais do arquivo, como nome, versão, tamanho, idioma, informações de certificado;
- 10.1.8.17. A solução de EDR deve ser integrada ao agente de antivírus, instalada como um agente único em estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;
- 10.1.8.18. O gerenciamento da solução de EDR deve ser feito a partir da mesma Console de Gerenciamento da solução antivírus;
- 10.1.8.19. Deve fornecer guias de respostas a incidentes, fornecendo visibilidade sobre o escopo de um ataque, como ele começou, o que foi impactado, e como responder;
- 10.1.8.20. Deve responder ao incidente com opção de isolamento da máquina, bloqueio e limpeza da ameaça;
- 10.1.8.21. Deve realizar buscas de ameaças em todo o ambiente, permitir buscar por *Hash*, nome, endereços IP, domínio ou linha de comando;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 10.1.8.22. Funcionalidade de Controle de Aplicações e Dispositivos Externos:
- 10.1.8.23. Possuir controle de aplicativos para monitorar e impedir que os usuários executem ou instalem aplicações que podem afetar a produtividade ou o desempenho da rede;
- 10.1.8.24. Atualizar automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicativos específicos ou categorias específicas de aplicações possam ser liberadas ou bloqueadas;
- 10.1.8.25. Verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões. Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web;
- 10.1.8.26. Oferecer proteção para chaves de registro e controle de processos;
- 10.1.8.27. Proibir através de política a inicialização de um processo ou aplicativo com base no nome e no *Hash* do arquivo;
- 10.1.8.28. Detectar um aplicativo controlado quando os usuários o acessarem, com as opções de permitir e alertar ou bloquear e alertar;
- 10.1.8.29. Possuir a opção de customizar uma mensagem a ser mostrada ao usuário em caso de bloqueio de execução do aplicativo;
- 10.1.8.30. Gerenciar o uso de dispositivos de armazenamento USB (ex: pen-drives e HDs USB). Permitir, através de regras, o bloqueio ou liberação da leitura/escrita/execução do conteúdo desses dispositivos;
- 10.1.8.31. Controlar o uso de outros dispositivos periféricos, como comunicação infravermelha e modem externo;
- 10.1.8.32. As funcionalidades do Controle de Aplicações e Dispositivos deverão ser nativas do produto ou incorporadas automaticamente por meio de *Plugins* sem utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante;
- 10.1.8.33. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
- 10.1.8.34. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
- 10.1.8.35. A gestão desses dispositivos deve ser feita diretamente na Console de Gerenciamento, deve permitir definir políticas diferentes por grupos de *Endpoints*;
- 10.1.8.36. Permitir a autorização de um dispositivo com no mínimo as seguintes opções:
- Permitir que todos os dispositivos do mesmo modelo;
 - Permitir que um único dispositivo com base em seu número de identificação único;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- c) Permitir o acesso total;
- d) Permitir acesso somente leitura.

10.1.9. Funcionalidades Contra-Ataques Avançados, Detecção e Resposta.

- 10.1.9.1. A solução deve ter capacidade de implementar técnicas avançada contra-ataque, detecção e resposta, possibilitando detecção e investigação nas estações de trabalho com atividades suspeitas;
- 10.1.9.2. Em caso de incidente a solução deve mostrar a trilha da infecção de forma visual, mostrando o início, todas as interações do *Malware* e o ponto final de bloqueio.
- 10.1.9.3. Após a análise da nuvem de inteligência do fabricante a solução deve apresentar um relatório sobre a ameaça contendo no mínimo:
- 10.1.9.4. Detalhes do Processo, como nome, *Hash*, hora e data da detecção e remediação;
- 10.1.9.5. Reputação do arquivo e correlação da detecção do arquivo em outras soluções de antivírus através de bases de conhecimento como o Vírus Total ou do próprio fabricante;
- 10.1.9.6. Resultado da análise do arquivo suspeito pela funcionalidade de *Machinne Learning* ou *Deep Learning*;
- 10.1.9.7. Propriedades gerais do arquivo, como nome, versão, tamanho, idioma, informações de certificado;
- 10.1.9.8. A solução de EDR (*Endpoint Detection and Response*) deve ser integrada ao agente de antivírus, instalada como um agente único em estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;
- 10.1.9.9. O gerenciamento da solução de EDR deve ser feito a partir da mesma console de gerenciamento da solução antivírus;
- 10.1.9.10. Deve fornecer guias de respostas a incidentes, fornecendo visibilidade sobre o escopo de um ataque, como ele começou, o que foi impactado, e como responder;
- 10.1.9.11. Deve responder ao incidente com opção de isolamento da máquina, bloqueio e limpeza da ameaça;
- 10.1.9.12. Deve realizar buscas de ameaças em todo o ambiente, permitir buscar por *Hash*, nome, endereços IP, domínio ou linha de comando;
- 10.1.10. Funcionalidade de Controle de Aplicações e Dispositivos:
 - 10.1.10.1. Oferecer proteção para chaves de registro e controle de processos;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 10.1.10.2. Proibir, através de política a inicialização de um processo ou aplicativo, com base no nome e no *Hash* do arquivo;
- 10.1.10.3. Gerenciar o uso de dispositivos de armazenamento USB (ex: pen-drives e HDs USB). Permitir, através de regras, o bloqueio ou liberação da leitura/escrita/execução do conteúdo desses dispositivos;
- 10.1.10.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
- 10.1.10.5. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
- 10.1.10.6. A gestão desses dispositivos deve ser feita diretamente na console de gerenciamento e permitir definir políticas diferentes por grupos de *Endpoints*;
- 10.1.10.7. Permitir a autorização de um dispositivo com no mínimo as seguintes opções:
- a) Permitir todos os dispositivos do mesmo modelo;
 - b) Permitir um único dispositivo com base em seu número de identificação único;
 - c) Permitir o acesso total;
 - d) Permitir acesso somente leitura.
- 10.1.10.8. Proteger servidores contra *Malwares*, arquivos e tráfego de rede malicioso, controle de periféricos, controle de acesso à web, controle de aplicativos em um único agente instalado nos servidores;
- 10.1.10.9. Realizar a pré-execução do agente para verificar o comportamento malicioso e detectar *Malwares* desconhecidos;
- 10.1.10.10. O agente *Host* deve buscar algum sinal de *Malwares* ativos e detectar *Malwares* desconhecidos;
- 10.1.10.11. O agente deve realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes;
- 10.1.10.12. A solução deve manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência;
- 10.1.10.13. Realizar a verificação de todos os arquivos acessados em tempo real, mesmo durante o processo de *Boot*;
- 10.1.10.14. Realizar a verificação de todos os arquivos no disco rígido em intervalos programados;
- 10.1.10.15. Realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

e aplicações potencialmente indesejáveis (PUA);

- 10.1.10.16. Proteger os navegadores Internet Explorer, Firefox, Chrome, Opera, Safari e Microsoft Edge, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados;
- 10.1.10.17. Permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos;
- 10.1.10.18. É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, *Spyware*, *Trojans*, *Worms*, *Adware* e aplicativos potencialmente indesejados (PUAs);
- 10.1.10.19. O cliente para instalação em servidores deve ser compatível com os sistemas operacionais abaixo:
 - a) Windows Server 2022;
 - b) Windows Server 2019;
 - c) Windows Server 2016;
 - d) Windows Server 2012 R2 (64 bit);
 - e) Windows Server 2012 (64 bit);
 - f) Windows Server 2008 R2 (64 bit);
 - g) Ubuntu (versão atual 20.04 ou superior).
- 10.1.10.20. Suportar a inclusão de outros servidores para a função de atualização distribuída e cache, de forma a agilizar o processo de atualização dos demais agentes;
- 10.1.10.21. Possuir integração com as nuvens da Microsoft Azure e Amazon Web Services para identificar as informações dos servidores instanciados nas nuvens;
- 10.1.10.22. Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção;
- 10.1.10.23. Permitir a utilização de senha de proteção para permitir a reconfiguração local no cliente ou desinstalação dos componentes de proteção;
- 10.1.10.24. Funcionalidade de *Firewall* e Detecção e Proteção de Intrusão (IDS/IPS);
- 10.1.10.25. Possuir proteção contra exploração de *Buffer Overflow*;
- 10.1.10.26. Possuir proteção contra-ataques de Negação de Serviço (Denial of Service - DoS), Port-Scan, MAC Spoofing e IP Spoofing;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 10.1.10.27. Possuir atualização periódica de novas assinaturas de ataque;
- 10.1.10.28. Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (*Hash*) do arquivo.
- 10.1.10.29. Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas;
- 10.1.10.30. Possuir um sistema de prevenção de intrusão no *Host* (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados.
- 10.1.10.31. Identificar comportamentos suspeitos de códigos e ataques de dia zero (*Zero Day*), tais como: *Buffer Overflow*, tráfego de códigos maliciosos e atividades suspeitas detectadas por comportamento.
- 10.1.10.32. Possuir técnicas de proteção, que inclui:
- Análise dinâmica de código - técnica para detectar *Malware* criptografado mais complexo;
 - Algoritmo correspondente padrão - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificado como um vírus;
 - Possuir capacidade para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;
 - Possuir tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo. jpg.txt) ou a extensão não coincida com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt);
 - Verificação de ameaças *Web* avançadas: bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise comportamental para identificar e parar o código malicioso de *Malware* avançados.
- 10.1.11. Funcionalidade de Antivírus e *AntiSpyware*:
- 10.1.11.1. Proteção em tempo real contra vírus, *Trojans*, *Worms*, *Rootkits*, *Botnets*, *Spyware*, *Adwares* e outros tipos de códigos maliciosos.
- 10.1.11.2. Proteção *Anti-Malware* nativa da solução ou incorporada automaticamente por meio de *Plug-Ins* sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante.
- 10.1.11.3. As configurações do *Anti-Spyware* devem ser realizadas através da mesma console do

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

antivírus;

- 10.1.11.4. Permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou *Malware*, permitir a inclusão de arquivos em listas de exclusão (*Whitelists*) para que não sejam verificados pelo produto;
- 10.1.11.5. Permitir a varredura das ameaças da maneira manual, agendada e em tempo real nos servidores;
- 10.1.11.6. Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do antivírus;
- 10.1.11.7. Capacidade de detectar arquivos através da reputação dos mesmos;
- 10.1.11.8. Capacidade de remoção automática total dos danos causados por *Spyware*, *Adwares* e *Worms*, como limpeza do registro e pontos de carregamento, com opção de finalizar o processo e terminar o serviço da ameaça no momento de detecção;
- 10.1.11.9. A remoção automática dos danos causados deve ser nativa do próprio antivírus; ou adicionada por *Plugin*, desde que desenvolvido ou distribuído pelo fabricante;
- 10.1.11.10. Bloquear origem de infecção através de compartilhamento de rede com opção de bloqueio da comunicação via rede;
- 10.1.11.11. Detectar tráfego de rede para comandar e controlar os servidores;
- 10.1.11.12. Proteger arquivos de documento contra-ataque do tipo *Ransomwares*;
- 10.1.11.13. Proteger contra ataques de *Ransomware* em pastas compartilhadas na rede;
- 10.1.11.14. Permitir o envio de amostras de *Malwares* para a nuvem de inteligência do fabricante;
- 10.1.11.15. Permitir o bloqueio da verificação de vírus em recursos mapeados da rede;
- 10.1.11.16. Antivírus de *Web* (verificação de *Sites* e *Downloads* contra vírus).
- 10.1.12. Gerenciamento e administração centralizada
 - 10.1.12.1. A console de monitoração e configuração deve ser feita através de uma central para o grupo de *Anti-Malware*, baseada em *Web* e em nuvem ou *Appliance*, que deve conter todas as ferramentas para a monitoração e controle da proteção dos dispositivos;
 - 10.1.12.2. A console deve apresentar painel com o resumo dos *Status* de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 10.1.12.3. Possuir mecanismo de comunicação via API, Syslog ou RESTFULL API (*Representational State Transfer*), para integração com outras soluções de segurança, disponibilizando acesso a documentação técnica da API do fabricante;
- 10.1.12.4. A console deve permitir a divisão dos computadores, dentro da estrutura de gerenciamento em grupos;
- 10.1.12.5. Permitir sincronização com o *Active Directory* (AD) para gestão de usuários e grupos integrados às políticas de proteção.
- 10.1.12.6. Aplicar regras diferenciadas baseado em grupos ou usuários;
- 10.1.12.7. A instalação deve ser feita via cliente específico por *Download* da gerência central ou também via *Email* de configuração. O instalador deve permitir a distribuição do cliente via *Active Directory* (AD) para múltiplas máquinas;
- 10.1.12.8. A console deve permitir criar e editar diferentes políticas para a aplicação das proteções exigidas e aplicadas a nível de usuários ou *Endpoint*, não importando em que equipamentos eles estejam acessando;
- 10.1.12.9. Fornecer atualizações do produto e das definições de vírus e proteção contra intrusos;
- 10.1.12.10. Permitir exclusões de escaneamento para um determinado *Website*, pasta, arquivo ou aplicação, tanto a nível geral quanto específico em uma determinada política.
- 10.1.12.11. A console de gerenciamento deve permitir a definição de grupos de usuários com diferentes níveis de acesso as configurações, políticas e *Logs*;
- 10.1.12.12. Atualização incremental, remota e em tempo-real, da vacina dos antivírus e do mecanismo de verificação (*Engine*) dos clientes;
- 10.1.12.13. Permitir o agendamento da varredura contra vírus, permitir selecionar uma máquina, grupo de máquinas ou domínio, com periodicidade definida pelo administrador;
- 10.1.12.14. Atualização automática das assinaturas de ameaças (*Malwares*) e políticas de prevenção desenvolvidas pelo fabricante em tempo real ou com periodicidade definida pelo administrador;
- 10.1.12.15. Utilizar protocolos seguros padrão HTTPS para comunicação entre console de gerenciamento e clientes gerenciados.
- 10.1.12.16. As mensagens geradas pelo agente devem estar no idioma em português ou permitir a sua edição.
- 10.1.12.17. Recursos do relatório e monitoramento devem ser nativos da própria console central de gerenciamento;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 10.1.12.18. Exibir informações como nome da máquina, versão do antivírus, sistema operacional, versão da *Engine*, data da vacina, data da última verificação, eventos recentes e *Status*;
- 10.1.12.19. Capacidade de geração de relatórios, estatísticos ou gráficos, tais como:
- 10.1.12.20. Detalhar quais usuários estão ativos, inativos ou desprotegidos, bem como detalhes dos mesmos;
- 10.1.12.21. Detalhamento dos computadores que estão ativos, inativos ou desprotegidos, bem como detalhes das varreduras e dos alertas nos computadores;
- 10.1.12.22. Detalhamento dos periféricos permitidos ou bloqueados, bem como detalhes de onde e quando cada periférico foi usado;
- 10.1.12.23. Detalhamento das principais aplicações bloqueadas e os servidores/usuários que tentaram acessá-las;
- 10.1.12.24. Detalhamento das aplicações permitidas que foram acessadas com maior frequência e os servidores/usuários que as acessam;
- 10.1.12.25. Detalhamento dos servidores/usuários que tentaram acessar aplicações bloqueadas com maior frequência e as aplicações que eles tentaram acessar;
- 10.1.12.26. Detalhamento de todas as atividades disparadas por regras de prevenção de perda de dados.
- 10.1.12.27. Possuir um elemento de comunicação para mensagens e notificações entre estações e a console de gerenciamento utilizando comunicação criptografada;
- 10.1.12.28. Fornecer solução de gerenciamento de arquivos armazenados em nuvem, garantindo que um arquivo que foi feito um *Upload* (exemplo Dropbox, Google Drive, OneDrive), tenha o processo monitorado e gerenciado, bem como realizar automaticamente o escaneamento do arquivo contra *Malwares*, procuradas palavras chaves ou informações confidenciais. Deve ser bloqueado o *Upload* ou removida a informação confidencial antes do envio do arquivo;
- 10.1.12.29. As portas de comunicação deverão ser configuráveis. A comunicação deve permitir QoS para controlar a largura de banda de rede.
- 10.1.12.30. A solução deve permitir a seleção da versão do *Software* de preferência, permitindo assim o teste da atualização sobre um grupo de PCs piloto antes de implantá-lo para toda a rede. Permitir ainda selecionar um grupo de computadores para aplicar a atualização para controlar a largura de banda de rede. A atualização da versão deve ser transparente para os usuários finais.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 10.1.12.31. O agente antivírus deve proteger *Laptops*, *Desktops* e servidores em tempo real, sob demanda ou agendado para detectar, bloquear e limpar todos os vírus, *Trojans*, *Worms* e *Spyware*. No Windows o agente também deve detectar PUA, *Adware*, comportamento suspeito, controle de aplicações e dados sensíveis. O agente ainda deve fornecer controle de dispositivos terceiros e, controle de acesso à web;
- 10.1.12.32. Possuir mecanismo contra a desinstalação do *Endpoint* pelo usuário e cada dispositivo deve ter uma senha única;
- 10.1.12.33. Prover no *Endpoint* a solução de HIPS (*Host Intrusion Prevention System*) para a detecção automática e proteção contra comportamentos maliciosos (análise de comportamento) e deve ser atualizado diariamente;
- 10.1.12.34. Prover proteção automática contra *Web Sites* infectados e maliciosos, assim como prevenir o ataque de vulnerabilidades de *Browser* via *Web Exploits*;
- 10.1.12.35. Permitir a monitoração e o controle de dispositivos removíveis nos equipamentos dos usuários, como dispositivos USB, periféricos da própria estação de trabalho e redes sem fio;
- 10.1.12.36. O controle de dispositivos deve ser ao nível de permissão, somente leitura ou bloqueio;
- 10.1.12.37. A ferramenta de administração centralizada deve gerenciar todos os componentes da proteção para estações de trabalho e servidores e deve ser projetada para a fácil administração, supervisão e elaboração de relatórios dos *Endpoint* e servidores;
- 10.1.12.38. Possuir interface gráfica *Web*, com suporte a língua portuguesa (padrão brasileiro);
- 10.1.12.39. A Console de administração deve incluir um painel com um resumo visual em tempo real para verificação do *Status* de segurança;
- 10.1.12.40. Fornecer filtros pré-construídos que permitam visualizar e corrigir apenas os computadores que precisam de atenção;
- 10.1.12.41. Exibir os PCs gerenciados de acordo com critérios da categoria (detalhes do estado do computador, detalhes sobre a atualização, detalhes de avisos e erros, detalhes do antivírus etc.), e classificar os PCs em conformidade;
- 10.1.12.42. Uma vez que um problema seja identificado, permitir corrigir os problemas remotamente, com no mínimo as opções abaixo:
- Proteger o dispositivo com a opção de início de uma varredura;
 - Forçar uma atualização naquele momento;
 - Ver os detalhes dos eventos ocorridos;
 - Executar verificação completa do sistema;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- e) Forçar o cumprimento de uma nova política de segurança;
- f) Mover o computador para outro grupo;
- g) Apagar o computador da lista.

10.1.12.43. Atualizar a políticas de segurança quando um computador for movido de um grupo para outro manualmente ou automaticamente;

10.1.12.44. Permitir exportar o relatório de *Logs* de auditoria nos formatos CSV e PDF;

10.1.12.45. Deve conter vários relatórios para análise e controle dos usuários e *Endpoints*. Os relatórios deverão ser divididos, no mínimo, em relatórios de: eventos, usuários, controle de aplicativos, periféricos e *Web*, indicando todas as funções solicitadas para os *Endpoints*;

10.1.12.46. Fornecer relatórios utilizando listas ou gráficos, utilizando informações presentes na console, com no mínimo os seguintes tipos:

- a) Nome do dispositivo;
- b) Início da proteção;
- c) Último usuário logado no dispositivo;
- d) Último *Update*;
- e) Último escaneamento realizado;
- f) *Status* de proteção do dispositivo;
- g) Grupo a qual o dispositivo faz parte;

10.1.12.47. Permitir a execução manual de todos estes relatórios nos formatos CSV e PDF;

10.2. PROCESSO DE EXECUÇÃO DO SERVIÇO MONITORAMENTO, DETECÇÃO E RESPOSTA A INCIDENTES PARA ENDPOINTS

10.2.1. O gerenciamento da solução de segurança Endpoint Security deverá contemplar as atividades listadas abaixo.

10.2.1.1. Administração da solução de Endpoint Security seguindo as melhores práticas do fabricante da solução;

10.2.1.2. Configuração da console de gerência;

10.2.1.3. Realizar health check mensal na plataforma para otimizar configurações de forma corretiva ou preventiva visando a redução de riscos de segurança e elevação do nível de maturidade;

10.2.1.4. Instalar, configurar e documentar novos componentes ou novas funcionalidades que

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

estiverem disponíveis no produto;

- 10.2.1.5. Customizar relatórios nativos a partir da solução de gerência da solução de Endpoint Security;
- 10.2.1.6. Instalação remota dos agentes nos dispositivos (servidores e desktops e notebooks).
- 10.2.1.7. Identificar e corrigir de forma proativa ou corretiva problemas na eficácia do endpoint gerenciado;
- 10.2.1.8. Integrar a solução com o ambiente do cliente utilizando integrações nativas que não dependam de desenvolvimento, como por exemplo, autenticação LDAP, envio de alertas de e-mails via relay;
- 10.2.1.9. Configurar alertas e notificações na plataforma, conforme alinhamento com o cliente;
- 10.2.1.10. Corrigir falhas e problemas que impactem nas funcionalidades ou disponibilidade da aplicação que não dependam diretamente da infraestrutura local como acesso à internet, falhas de comunicação decorrentes de falhas de rede, falhas no sistema de virtualização etc.;
- 10.2.1.11. Notificar o cliente sempre que houver novas versões do produto, elaborar documento de implantação para execução do upgrade e realizar upgrade da solução após aprovação formal do cliente;
- 10.2.1.12. Apoiar na criação das rotinas de backup e restore da solução em casos de desastres seguindo as recomendações e melhores práticas do fabricante da solução;
- 10.2.1.13. Em casos de incidentes de segurança que impactem o funcionamento da solução de Endpoint Security a CONTRATADA deverá apoiar na reconstrução do ambiente administrado por este contrato;
- 10.2.1.14. Atender a requisições de serviço que tratem de dúvidas sobre funcionalidade ou configurações do produto adquirido neste contrato;
- 10.2.1.15. Realizar reuniões mensais para acompanhamento dos resultados;
- 10.2.1.16. Acionar equipe de Segurança da Informação da CONTRATANTE para auxiliar em diagnóstico e tratamento de problemas de maior complexidade e impacto;
- 10.2.1.17. Certificar diariamente que as atualizações de vacinas estejam sendo recebidas e distribuídas para o parque de ativos;
- 10.2.1.18. Definir e manter atualizado os procedimentos operacionais relacionados a solução listados abaixo.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 10.2.1.18.1. Troubleshooting de comunicação.
- 10.2.1.18.2. Troubleshooting de vacinas.
- 10.2.1.18.3. Troubleshooting de funcionamento do agente.
- 10.2.1.18.4. Procedimento de instalação do agent.
- 10.2.1.18.5. Tratamento de incidentes relacionados a solução de Endpoint Security.

10.2.2. ENTREGAS A SEREM REALIZADAS

10.2.2.1. Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, o CONTRATANTE definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue de forma on line e em tempo de execução, através do portal de indicadores descrito no tópico de condições gerais para prestação do serviço deste termo de referência, a saber:

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Ameaças identificadas na solução de endpoint Security	Soma de ameaças	Ameaças	Ameaças	Número total de Ameaças
Conformidade de assinaturas nos endpoints gerenciados	Soma de não conformidade	Tipos com maior frequência	Conformidade	Número total de não conformidade por tipo
Cobertura de proteção dos endpoints descoberto vs instalado	Soma de divergência	Protegido	Protegidos	% do parque protegido

Tabela 6 - Indicadores Estratégicos de Monitoramento de EndPoints

11. DO PAGAMENTO DOS SERVIÇOS

- 11.1. A prestação dos serviços será baseada no modelo de remuneração em função dos resultados apresentados, em que os pagamentos serão feitos após mensuração do Nível Mínimo de Serviço (NMS) definido em contrato/Termo de Referência, de modo a resguardar a eficiência e a qualidade na prestação dos serviços.
- 11.2. Os pagamentos terão início somente após a instalação da solução e a completa disponibilização dos serviços, mediante o aceite definitivo da CONTRATANTE.
 - 11.2.1. O CRCMG efetuará o pagamento em até 10 (dez) dias úteis, contados a partir do recebimento da Nota Fiscal com as devidas deduções legais.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 11.2.2. Considera-se ocorrido o recebimento da nota fiscal ou fatura no momento em que o CRCMG contratante atestar a execução do objeto do contrato.
- 11.2.3. A Nota Fiscal deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da Lei nº 8.666, de 1993.
- 11.3. Serão descontados sobre o pagamento a ser realizado, as devidas retenções de tributos e contribuições, conforme determina a Instrução Normativa nº. 1.234, de 11/01/2012, da Secretaria da Receita Federal.
- 11.4. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para o CRCMG.
- 11.5. Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.
- 11.6. Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do CRCMG.
- 11.7. Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018.
- 11.8. Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.
- 11.9. Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.
- 11.10. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.
- 11.11. Será rescindido o contrato em execução com a contratada inadimplente no SICAF, salvo por motivo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 11.12. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

$$I = (TX) \quad I = \frac{(6 / 100)}{365} \quad TX = \text{Percentual da taxa anual} = 6\% \\ I = 0,00016438$$

- 11.13. Os preços são fixos e irreajustáveis no prazo de um ano contado da data limite para a apresentação das propostas.

- 11.14. Dentro do prazo de vigência do contrato e mediante solicitação da contratada, os preços contratados poderão sofrer reajuste após o interregno de um ano, aplicando-se o índice IPCA acumulado nos 12 (doze) meses anteriores a data base ou outro índice que venha a substituí-lo, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

- 11.15. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

12. DA MENSURAÇÃO

- 12.1. O pagamento será feito mensalmente, levando-se em consideração o Nível Mínimo de Serviço (NMS) acordado em contrato, para o período de faturamento avaliado. O valor a ser pago será o valor unitário do item correspondente, alinhado com o NMS previsto em contrato.

- 12.2. Conforme ACORDO DE NÍVEIS DE SERVIÇO os SERVIÇOS GERENCIADOS DE SEGURANÇA serão medidos, nos seguintes termos:

- 12.2.1. DISPONIBILIDADE MENSAL DOS GRUPOS DE TECNOLOGIAS: Acompanha a execução do SERVIÇO DE GESTÃO DE DISPONIBILIDADE sobre os ativos de segurança, sob responsabilidade da CONTRATADA.

- 12.2.2. As qualificações técnicas exigidas para o perfil de analista(s) que participará do supracitado GRUPO DE DISPONIBILIDADE, da CONTRATADA:

Perfis	Certificações	Descrição
• Analista de Segurança I	• ITIL foundation V3 Ou	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

	ISFS (Information Security Foundation)	da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento pleno em segurança da informação, realizando monitoramento de disponibilidade de ambiente de segurança da informação, similares ao ambiente supracitado. Experiência comprovada de no mínimo 12 (doze) meses em tecnologia da informação.

Tabela 7 – Qualificações Grupo de Disponibilidade

- 12.2.3. No momento da assinatura do contrato, será exigido da CONTRATADA, a apresentação das documentações do(s) profissionais que participarão do GRUPO DE DISPONIBILIDADE, as quais devem comprovar as exigências e obrigações descritas neste termo de referência: contrato de prestação de serviços ou carteira de trabalho devidamente assinada pela CONTRATADA, para comprovação de habilidades, e as devidas certificações técnicas para comprovação do conhecimento conforme TABELA de exigências de qualificações.

12.2.4. ENTREGA MENSAL DOS SERVIÇOS:

- 12.2.4.1. Acompanha a execução de todos os demais serviços que compõem o objeto SERVIÇOS GERENCIADOS DE SEGURANÇA, sobre os ativos de segurança sob responsabilidade da CONTRATADA.

TIPO DE PRIORIDADE	QUANTIDADE DE ATENDIMENTO REALIZADO NO PERÍODO	QUANTIDADE DE ATENDIMENTO DESACORDO COM O NMS	FATOR DE ABATIMENTO POR DESEMPENHO DE SERVIÇO
P1			
P2			
P3			
P4			
P5			
P6			
P7			
P8			
VTAD (Valor R\$ total apurado)			

Tabela 8 – Dashboard de entrega de serviços

DENOMINAÇÃO	FORMA CÁLCULO	DE	FILTRO	AGRUPADOR
Tipo de prioridade	N/A		N/A	N/A

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

Quantidade de atendimento realizado no período	Soma de todos os atendimentos realizados no período	Período de apuração	Prioridade
Quantidade de atendimento desacordo com o NMS	Soma de todos os atendimentos realizados no período que não estão em conformidade com o NMS supracitado	Período de apuração	Prioridade
Fator de abatimento por desempenho de serviço (FADS)	Conforme item ENTREGA MENSAL DOS SERVIÇOS GERENCIADOS DE SEGURANÇA	Período de apuração	Prioridade
VTAD (Valor R\$ total apurado)	Soma do total de FADS, e subtrai do valor total previsto para o período	Período de apuração	N/A

Tabela 9 – Legenda de entrega de serviços

- 12.3. A reunião mensal deverá ocorrer até o 5º (quinto) dia útil após o término do período de faturamento, que coincidirá com o mês legal, e a disponibilidade dos relatórios será condição necessária ao recebimento dos serviços pelo CONTRATANTE. O primeiro mês de faturamento será parcial e proporcional, contado da data da emissão do termo de recebimento definitivo até o último dia do mês. Neste contexto, o profissional deve apresentá-lo de forma virtual, por meio de solução de videoconferência.
- 12.4. A respectiva nota fiscal/fatura, já deduzidos os fatores de abatimento calculados, deverá ser emitida somente após o recebimento definitivo dos serviços, e após a homologação das informações apresentadas pela CONTRATADA ao CONTRATANTE.
- 12.5. Caso não haja concordância da CONTRATADA com os fatores de abatimento calculados, os mesmos serão convertidos em sanção, aplicação de multa de mesmo valor, de forma a garantir o contraditório e a ampla defesa.
- 12.6. A qualquer tempo e a critério do CONTRATANTE, a bases dos sistemas utilizados para cálculo das entregas e indicadores listados neste tópico poderão ser solicitadas para auditorias e aferições.

13. DA ABRANGÊNCIA E ESCOPO DOS SERVIÇOS:

- 13.1. Considerar-se-á, para efeitos desta contratação, todos os recursos necessários para a perfeita execução efetiva da prestação dos serviços.
- 13.2. O dimensionamento da equipe para a execução adequada do serviço contratado é de responsabilidade exclusiva da CONTRATADA, devendo ser suficiente para o cumprimento integral dos níveis de serviço exigidos neste Termo de Referência.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

13.3. Dependendo da complexidade, criticidade e do prazo do projeto, os serviços poderão ser realizados nas instalações da CONTRATADA ou da CONTRATANTE.

13.4. Todos os custos com licenças de simuladores, *Softwares* devem estar contabilizados no valor do serviço, não sendo permitido o pagamento de valores adicionais ou extras, seja a que título for.

14. EXECUÇÃO DOS SERVIÇOS

14.1. A contratada deverá cumprir o seguinte cronograma de implantação dos serviços:

CRONOGRAMA DE IMPLANTAÇÃO		
ITENS	SERVIÇOS PREVISTOS:	PRAZO
1	Reunião de início de projeto (Kick-Off). Deverá ser previamente agendada pela CONTRATADA com até 02 (dois) dias úteis de antecedência.	10*
2	Entrega do Projeto Executivo pela CONTRATADA , a partir da reunião de início do projeto (Kick-Off).	30*
3	Manifestação de reajustes pela CONTRATANTE , se for o caso, a partir da data de entrega do Projeto Executivo.	10*
4	Ajustes, se for o caso, no Projeto Executivo pela CONTRATADA , a partir da manifestação de reajustes pela CONTRATANTE .	10*
5	Centro de Operações de Segurança da CONTRATADA em pleno funcionamento e operação em regime 24x7x365, a partir da data de início da vigência do contrato.	75*
6	Conclusão da fase de implantação dos serviços, contados a partir da data de início da vigência do contrato. Após a emissão do termo de recebimento definitivo pela CONTRATANTE .	90*
7	Disponibilidade dos serviços pela CONTRATADA .	60 meses**

Tabela 10 – Cronograma de implantação

* Prazos em dias corridos contados da data de assinatura do contrato.

** Prazo em meses contado a partir da assinatura do contrato.

14.2. A CONTRATADA deverá atender às seguintes condições gerais para início da prestação de cada um dos serviços, incluindo fase de concepção da solução, confecção de Projeto Executivo, planejamento de atividades de instalação, customização de ambiente e ativação de serviços sem ônus adicionais ao CONTRATANTE:

14.2.1. Reunião de início do projeto (*Kick-Off*), a ser realizada em até 10 (dez) dias corridos após a assinatura do contrato, a ser previamente agendada pela CONTRATADA com 02 (dois) dias úteis de antecedência.

14.2.1.1. A reunião deverá ser realizada preferencialmente de forma remota.

14.2.2. Serão de responsabilidade da CONTRATADA as atividades de instalação, integração,

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

configuração e testes de todos os produtos componentes de cada solução alocada, excluindo-se a Solução de Segurança da CONTRATANTE já ativa (Firewall), em conformidade com o Projeto Executivo a ser elaborado e apresentado pela CONTRATADA para prévia aprovação pela CONTRATANTE;

- 14.2.3. A CONTRATADA deverá levantar informações acerca dos locais de instalação dos produtos durante a elaboração do Projeto Executivo, e, se necessário, efetuar visita técnica para verificar eventuais requisitos físicos a serem providos para a correta instalação e prestação dos serviços;
- 14.2.4. A elaboração do Projeto Executivo é de responsabilidade da CONTRATADA e deverá conter as fases do projeto, os cronogramas de execução, e a descrição detalhada dos produtos e subprodutos a serem entregues em cada fase.
 - 14.2.4.1. A conclusão da fase de implantação dos serviços é de até 90 (noventa) dias corridos, contados a partir da data de assinatura do contrato, iniciando-se, a partir de então, a fase de prestação mensal dos serviços, apenas após a emissão do termo de recebimento definitivo.
- 14.2.5. Conter a descrição de topologia lógico e física da rede atual e topologia pretendida em cada etapa;
- 14.2.6. Efetuar o mapeamento de criticidade de todos os ativos envolvidos no projeto, inclusive os de propriedade da CONTRATANTE;
- 14.2.7. Para a implantação dos serviços, indicar de forma detalhada as condições de *Rollback* de cada mudança no ambiente da CONTRATANTE;
- 14.2.8. Estimar o consumo de Unidades de *Rack* (U) e de energia de cada ativo a ser instalado nas dependências da CONTRATANTE, se for o caso;
- 14.3. Os *Softwares* e demais componentes necessários à correta prestação dos serviços deverão:
 - 14.3.1. Conter os recursos necessários e estarem configurados de modo a garantir total operabilidade no ambiente computacional da CONTRATANTE e otimizados para usufruir das melhores condições em termos de desempenho e disponibilidade;
 - 14.3.2. Conter a última versão de *Software* e *Firmware* homologado pelo fabricante;
 - 14.3.3. Ter configuradas senhas de acesso para que a equipe de funcionários designados pelo CONTRATANTE efetue o acesso para a visualização das configurações e *Logs* (acesso seguro e remoto);
 - 14.3.4. Ter configurada senha com direitos totais de administração e configuração a ser utilizada pela CONTRATANTE em caso de emergência;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 14.4. Para aprovação da instalação e configuração de qualquer item que ensejar a emissão de termo de recebimento definitivo, a CONTRATADA deve elaborar relatório técnico com análise dos resultados e impactos decorrentes da atividade executada;
- 14.5. Quando realizadas no ambiente de produção, as atividades poderão ser agendadas para serem executadas após o horário de expediente, a saber, em horários noturnos – após às 20h00 (vinte horas) – além de finais de semana e feriados, conforme disponibilidade da CONTRATANTE;
- 14.6. A operação assistida deverá obedecer aos requisitos a seguir:
- 14.6.1. Iniciará quando forem finalizados o planejamento, a customização de ambiente e a instalação dos ativos de rede, sendo o item de serviço submetido para recebimento definitivo.
- 14.6.2. A mudança para o ambiente de produção será concomitante a este momento, salvo se expressamente solicitado pela CONTRATANTE que seja feita em data diferente. Terá duração de até 30 (trinta) dias corridos, e será executada em Belo Horizonte-MG, nas dependências da CONTRATANTE, em horário comercial (entre 8h30 e 17h30);
- 14.6.3. Caso seja necessária a consecução de atividades pelo técnico responsável pela operação assistida, e que possa afetar a disponibilidade de serviços do ambiente da CONTRATANTE, estas deverão ocorrer após às 20h00 (vinte) horas;
- 14.7. Caso a CONTRATANTE encontre pendências impeditivas à emissão do termo de recebimento definitivo, a operação assistida deverá ser prorrogada até que sejam sanados os motivos geradores das pendências;
- 14.8. Caso a implantação de um serviço cause interferência no funcionamento de qualquer funcionalidade na CONTRATANTE, a CONTRATADA deverá alocar profissionais com qualificação suficiente para corrigir o problema ou retornar o ambiente à condição anterior à implantação, sem quaisquer custos adicionais a CONTRATANTE.
- 14.9. Para todos os componentes da solução, a CONTRATADA deverá implementar e documentar as respectivas configurações de segurança necessárias, que visem à redução do risco de acesso indevido a cada servidor (*Hardening*), como, por exemplo, remoção de serviços desnecessários do sistema operacional, configurações de *Kernel*, configurações dos serviços ativos para suas permissões mínimas de funcionamento, remoção de usuários padrão de sistemas e aplicativos, além de eventuais configurações para resistir a ataques de negação de serviço.
- 14.10. Para o planejamento e o acompanhamento da instalação dos *Softwares* necessários à execução dos serviços, da entrega das etapas para recebimento definitivo, da confecção do Projeto Executivo, da confecção do as-built, e para as demais atividades pertinentes até a emissão do termo de recebimento definitivo de todos os itens, a CONTRATADA deverá alocar GERENTES DE PROJETOS.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

14.11. As qualificações técnicas mínimas exigidas para o perfil de GERENTE DE PROJETO da CONTRATADA são:

Certificações	Descrição
Ao menos uma das certificações de segurança da informação: • Project Management Professional (PMP); • Prince2 Practitioner Certificate in Project Management; • Professional Scrum Master I;	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em gerencia de projetos, com experiência mínima de 12 (doze) meses.

Tabela 11 – Qualificações do Gerente de Projeto

14.11.1. **No momento da assinatura do contrato** será exigido da CONTRATADA a apresentação das documentações do(s) profissional(is) com perfil de GERENTE DE PROJETO, as quais devem comprovar as exigências e obrigações descritas neste Termo de Referência: contrato de prestação de serviços ou carteira de trabalho devidamente assinada pela CONTRATADA, para comprovação de habilidades, e as devidas certificações técnicas para comprovação do conhecimento conforme TABELA de exigências de qualificações.

15. ACORDO DE NÍVEIS DE SERVIÇO

15.1. A prestação dos serviços será baseada no modelo de remuneração em função dos resultados apresentados, em que os pagamentos serão feitos após mensuração e verificação de métricas quantitativas e qualitativas, contendo indicadores de desempenho e metas, com Nível Mínimo de Serviço (NMS) definido em contrato, de modo a resguardar a eficiência e a qualidade da prestação dos serviços.

15.2. Os níveis mínimos de serviço contratados serão registrados, monitorados e comparados às metas de desempenho e qualidade estabelecidas, em termos de prazo e efetividade, condição fundamental para realização dos pagamentos previstos.

15.3. De modo a facilitar a compreensão dos Níveis Mínimos de Serviço (NMS) dos Serviços Gerenciados de Segurança, são apresentadas, a seguir, exigências mínimas em termos de níveis de serviço que devem ser atendidas pela CONTRATADA na execução do contrato, a saber:

15.4. DISPONIBILIDADE MENSAL DOS GRUPOS DE TECNOLOGIAS

15.4.1. Para os itens 1 a 5 dos Serviços Gerenciados de Segurança, a Meta de Disponibilidade Mensal (MDM) por grupo de tecnologia deve ser de, no mínimo:

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

item	Grupo de Tecnologia	MDM (%)	FPI
1	Proteção de Dados e <i>Datacenter</i>	95	1,75
2	Proteção de Dados de <i>Endpoints</i>	95	1,5
4	Visibilidade de Rede e Controle de Incidentes	95	1,5

Tabela 12 – Meta de Disponibilidade Mensal

15.5. O SERVIÇO DE GESTÃO DE DISPONIBILIDADE foi arquitetado para garantir e medir a disponibilidade do parque de segurança da informação descrito neste Termo de Referência. Logo, o mesmo deverá ser utilizado para apurar a meta de disponibilidade mensal (MDM).

15.6. Em cada período avaliado, o cálculo do Percentual de Disponibilidade Mensal (PDM) por item de serviço deve ser calculado com a seguinte fórmula:

$$PDM_k = \frac{[TM - TI_k]}{TM} * 100$$

PDM_k = Percentual de Disponibilidade Mensal do k-ésimo item de serviço;

k = k-ésimo item de serviço;

TM = Tempo total mensal de operação, em minutos, no mês de faturamento;

TI_k = Tempo total mensal de indisponibilidade do k-ésimo item de serviço, em minutos, no mês de faturamento. Devem ser incluídos como Tempo de Indisponibilidade (TI_k):

15.7. Tempo em que o respectivo serviço esteja indisponível ou com desempenho degradado;

15.8. Tempo decorrente entre o início da indisponibilidade do serviço e a sua total recuperação;

15.9. Não devem ser incluídos como Tempo de Indisponibilidade (TI_k):

15.9.1. Falta de energia no local de prestação dos serviços;

15.9.2. Indisponibilidade da rede lógica da CONTRATANTE;

15.9.3. Problemas derivados de ocorrências no ambiente da CONTRATANTE, onde comprovadamente a indisponibilidade não esteja sendo controlada pela CONTRATADA;

15.9.4. Ações necessárias para resolução de problemas que tenham sido autorizadas pelo CONTRATANTE;

15.9.5. Indisponibilidade gerada pela operadora de telecomunicação responsável pelos *Links* e equipamentos do ambiente da CONTRATANTE;

15.9.6. Fatores externos a prestação de serviços, desde que justificado e acordado com o time de segurança da CONTRATANTE;

15.9.7. Indisponibilidade do ambiente virtualizado da CONTRATANTE, infraestrutura computacional em que parte dos *Softwares* que compõem a solução deve ser instalada;

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 15.9.8. Manutenções programadas pela CONTRATANTE;
- 15.9.9. Manutenções programadas pela CONTRATADA, desde que previamente autorizadas pela CONTRATANTE.
- 15.9.10. *Tickets* abertos cujo prazo de resolução encerre somente no próximo período de faturamento somente terão calculados os fatores de abatimento a partir do período seguinte;
- 15.10. Os fatores de abatimento por indisponibilidade de serviços (FAIS) relativos ao percentual de disponibilidade mensal deverão, ainda, ser multiplicados por um fator de peso do item (FPI), segundo a **Tabela** - META DE DISPONIBILIDADE MENSAL, por grupo de tecnologia.
- 15.11. O Percentual de Disponibilidade Mensal (PDM) é subsidiário para o cálculo do Fator de Abatimento por Indisponibilidade de Serviço (FAIS), desconto a ser aplicado no valor de prestação mensal de cada conjunto ou item de serviço;
- 15.12. Assim sendo, o Fator de Abatimento por Indisponibilidade de Serviço (FAIS) deve ser calculado de acordo com a seguinte fórmula:

$$FAIS = \sum_{k=1}^{10} VMI_k \times FPI_k \times \left\{ \frac{MDM_k - MIN(MDM_k, PD_k)}{100} \times MTI \right\}$$

Variável	Descrição
k	Número do grupo de tecnologia
FAIS	Fator de abatimento por indisponibilidade de serviço
VMI	Valor mensal do item de serviço de Gestão de Disponibilidade
MDM	Meta de disponibilidade mensal do item
PD	Percentual de disponibilidade mensal, calculada segundo fórmula supracitada.
MTI	Multiplicador por tempo de indisponibilidade, conforme definido a seguir: Valor = 1, se (MDM - PD) menor igual 1; Valor = 1, se (MDM - PD) maior que 1 e menor igual a 5; Valor = 1, se (MDM - PD) for maior que 5;
Min	Função que retorna o valor mínimo.

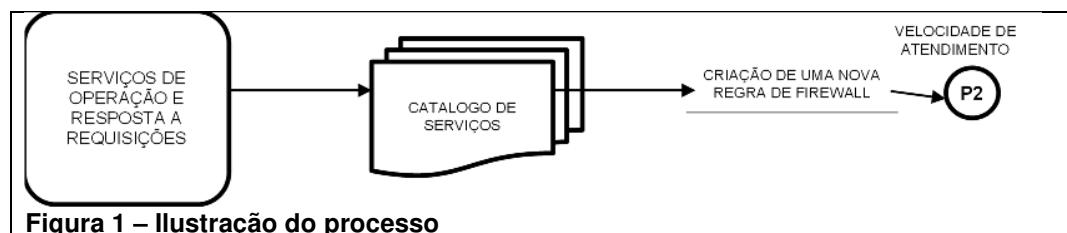
Tabela 13 – Variáveis de Cálculo de Fator de Abatimento por Indisponibilidade de Serviço (FAIS)

15.13. ENTREGA MENSAL DOS SERVIÇOS GERENCIADOS DE SEGURANÇA

- 15.13.1. Além da meta de disponibilidade mensal do parque de segurança da informação do CONTRATANTE, a qual avalia especificamente o **SERVIÇO DE GESTÃO DE DISPONIBILIDADE**, também deverão ser apurados os níveis de serviço para os demais serviços que, somados, compõem o objeto Serviços Gerenciados de Segurança.
- 15.13.2. Todos os serviços que compõem o objeto contratado possuem catálogo de serviço descrito no **ANEXO IV** deste Termo de Referência. Cada item (serviço) que compõe o catálogo de serviço deve estar relacionado com os tipos de velocidade de atendimento descritos na **Tabela**

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

3 deste termo de referência, conforme exemplo ilustrado na figura abaixo:



Tipos	Nível mínimo de serviço (NMS)	IndMeta	Fator de peso da Atividade (FAT)
P1	2 Horas	2 Horas	1
P2	4 Horas	4 Horas	1
P3	8 Horas	8 Horas	0,5
P4	16 Horas	16 Horas	0,5
P5	32 Horas	32 Horas	0,5
P6	64 Horas	64 Horas	0,25
P7	128 Horas	128 Horas	0,25
P8	256 Horas	256 Horas	0,25

Tabela 14 – Níveis de prioridade de Atendimento

- 15.13.3. Em um atendimento onde seja necessária uma janela para execução dos serviços solicitados, o tempo transcorrido entre a necessidade do atendimento e a janela de execução deverão ser excluídos.
- 15.13.4. Os fatores de abatimento por desempenho de serviço (FADS) serão calculados com base na comparação dos resultados alcançados na execução das atividades com os níveis de serviços definidos na TABELA 14 - NIVEIS DE PRIORIDADES DE ATENDIMENTO.
- 15.13.5. O FADS será calculado como somatório das ocorrências realizadas para cada uma das atividades definidas, conforme fórmula a seguir:

$$FADS = \sum_{i=1}^8 \sum_{j=1}^n VMC \times \left[\frac{\text{Max} (INDATINGi.j, INDMETAi) - INDMETAi}{10 \times INDMETAi} \right] \times FPAi$$

Variável	Descrição
I	Tipo de prioridade.
J	Contador de ocorrências do tipo de prioridade que não atenderam o NMS definido.
N	Quantidade de ocorrências do tipo de prioridade que não atenderam o NMS definido.
FADS	Fator de abatimento por desempenho de Serviço
VMC	Valor mensal do contrato.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

INDMETA	Índice de meta (NMS), em minutos/horas/dias, definido para a atividade.
INDATING	Índice atingido, em minutos/horas/dias, pela atividade que ultrapassou o (NMS).
FPA	Fator de peso da atividade.
Max	Função que retorna o valor máximo.

Tabela 15 – Variáveis de Cálculo de Fatores de Abatimento por Desempenho de Serviço (FADS)

16. PAPÉIS E RESPONSABILIDADES

16.1. Durante a vigência contratual, e toda a prestação do serviço objeto desta contratação, deverão ser observados e cumpridos os seguintes papéis e responsabilidades dos profissionais:

16.1.1. **Fiscal técnico do contrato (CONTRATANTE):** responsável pelo acompanhamento, fiscalização e avaliação da execução do objeto nos moldes contratados, observando o fiel cumprimento de todas as cláusulas contratuais.

16.1.2. **Gestor do contrato (CONTRATANTE):** responsável pela coordenação das atividades relacionadas à fiscalização, bem como dos atos preparatórios à instrução processual e da formalização dos procedimentos referentes aos aspectos que envolvam a prorrogação, a alteração, o reequilíbrio, o pagamento, eventuais aplicações de sanções e extinção dos contratos, dentre outras ações.

16.1.3. **Preposto (CONTRATADA):** é o profissional indicado pelo Fornecedor de Serviço para representá-la administrativa e tecnicamente. É o responsável pela coordenação operacional das atividades previstas nos projetos, de forma a solucionar qualquer dúvida, conflito ou desvio técnico que possa comprometer a execução das OS. Deverá ter bons conhecimentos em gestão de projetos para garantir o controle sobre os sinais vitais de cada projeto. Também é responsável pela interlocução com o Gestor do Contrato do CONTRATANTE.

16.2. As qualificações técnicas exigidas para o perfil de PREPOSTO da CONTRATADA:

Certificações	Descrição
Ao menos uma das certificações de segurança da informação: • CISSP (Certified Information Systems Security Professional); • CISM (Certified Information Security Manager); • CIA (Certified Intrusion Analyst), • GSEC (GIAC Security Essentials); • GCIH (GIAC Incident Handler) • GMON (GIAC Continuous Monitoring);	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência mínima de 12 (doze) meses em coordenação e gestão de contratos de serviços continuados.

Tabela 16 – Certificações e Qualificações do Preposto

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 16.3. **No momento da assinatura do contrato** será exigido da CONTRATADA a apresentação das documentações do(s) profissionais com perfil de PREPOSTO as quais devem comprovar as exigências e obrigações descritas neste termo de referência: contrato de prestação de serviços ou carteira de trabalho devidamente assinada pela CONTRATADA para comprovação de habilidades e as devidas certificações técnicas para comprovação do conhecimento conforme TABELA 16.

17. ESCOPO E PRAZOS DE EXECUÇÃO E DE ACEITE E NATUREZA DOS SERVIÇOS

- 17.1. O período de prestação dos serviços, a partir da emissão do termo de recebimento definitivo será o estabelecido na tabela abaixo:

LOTE	ITEM	DESCRIÇÃO	QTD	MÉTRICA	PERÍODO
1	1	Serviço de Monitoramento de Ataques Cibernéticos e Resposta A Incidentes	1	500 EPS*	60
	2	Serviço de Gestão de Vulnerabilidades	300	Ativos	60
	3	Serviço de Monitoramento, Detecção e Resposta a Incidentes para Endpoint	130	Ativos	60

*EPS - Eventos por Segundo - é uma métrica utilizada pelo mercado para dimensionar o SIEM (equipamento responsável pela coleta, análise e correlacionamento dos Logs).

- 17.2. SERVIÇOS GERENCIADOS DE SEGURANÇA – DEMANDA FUTURA serão demandados de acordo com as necessidades da CONTRATANTE, solicitados por meio de Ordem de Serviço cuja execução deve ser recebida por meio do Termo de Recebimento de Serviços.
- 17.3. A partir da assinatura do contrato, correrão os seguintes prazos:
- 17.4. Reunião de início do projeto (*Kick-Off*): a ser realizada em até 10 (dez) dias corridos após a assinatura do contrato. Deverá ser previamente agendada pela **CONTRATADA** com 02 (dois) dias úteis de antecedência.
- 17.5. Entrega do Projeto Executivo: até 30 (trinta) dias corridos, contados a partir da reunião de início do projeto (*Kick-Off*);
- 17.6. A CONTRATANTE se manifestará no prazo de até 10 (dez) dias corridos, contados da data de entrega do Projeto Executivo;
- 17.7. Havendo necessidade de ajustes, a CONTRATADA terá até 10 (dez) dias corridos para realizá-los, contados da notificação a ser efetuada pela CONTRATANTE, a respeito da manifestação sobre o Projeto Executivo;
- 17.8. A conclusão da fase de implantação dos serviços é de até 90 (noventa) dias corridos, contados a partir da data de início da vigência do contrato, mediante a emissão do termo de recebimento definitivo pela CONTRATANTE.
- 17.9. O termo de recebimento definitivo obedecerá os seguintes critérios:

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 17.10. A CONTRATANTE terá 15 (quinze) dias corridos para emitir o termo de recebimento definitivo depois de finalizado o planejamento, customização e a instalação do ambiente;
- 17.11. A prestação dos serviços mensais iniciará somente a partir da emissão do termo de recebimento definitivo pela CONTRATANTE;
- 17.12. Para todos os bens importados, caso necessário, por parte da CONTRATADA, que sejam instalados nas dependências da CONTRATANTE, será necessária a apresentação dos respectivos comprovantes de origem.
- 17.13. O Centro de Operações de Segurança da CONTRATADA deverão estar em pleno funcionamento, operando em regime 24x7x365, em até 75 (setenta e cinco) dias corridos, contados da data de início da vigência contratual.

18. INSPEÇÕES E DILIGÊNCIAS

- 18.1. A CONTRATANTE reserva-se o direito de efetuar inspeções e diligências para sanar quaisquer dúvidas existentes, podendo efetuá-las previamente à contratação;
- 18.2. A CONTRATANTE poderá realizar diligência no Centro de Operações de Segurança da CONTRATADA antes do início da prestação do serviço, *in loco*, a fim de validar e aferir se TODOS os itens solicitados neste Termo de Referência serão atendidos;
- 18.3. A contratação não será formalizada, caso **não** haja o atendimento de quaisquer itens previstos neste Termo de Referência.
- 18.4. As Diligências não poderão ser restritas a dias e horários específicos, sendo possível que a mesma seja executada em horários fora do chamado “horário comercial”, sendo possível a visitação em finais de semana, períodos noturnos e afins;
- 18.5. A CONTRATADA poderá restringir a quantidade de pessoas presentes na diligência, porém ela deverá apresentar durante a visita todas as comprovações necessárias, todos os processos solicitados e responder a todos os questionamentos.
- 18.6. Em caso de eventos adversos que impossibilitem a diligência a contratada deverá prover acesso de maneira remota e virtual para a verificação dos itens a serem inspecionados.

19. TRATAMENTO DE INCIDENTES CIBERNÉTICOS

- 19.1. É de responsabilidade da CONTRATADA a restauração dos serviços comprometidos através da definição de estratégias e de ações para conter o incidente; a erradicação dos artefatos maliciosos do ambiente do CRCMG; a recuperação dos serviços dependentes de tecnologia; bem como ações que terão como objetivo mitigar riscos existentes para evitar com que incidentes semelhantes ocorram no futuro.
- 19.1.1. É de responsabilidade da CONTRATANTE contactar as suas terceirizadas para atendimento

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

das estratégias e ações repassadas pela CONTRATADA para completo restabelecimento do ambiente o mais rápido e seguro.

19.1.1.1. Serviços de responsabilidade da CONTRATANTE:

- a) Restauração de Backups de servidores, serviços, dados, banco de dados, configurações do AD, senhas, GPOs, grupos;
- b) Configuração do Firewall;

19.2. Os serviços a serem executados, culminarão na entrega pela contratada dos seguintes documentos:

19.2.1. **Relatório executivo** – Demonstrará a conformidade e riscos antes da aplicação dos controles de segurança e após a aplicação dos controles de segurança;

19.2.2. **Relatório técnico** – Demonstrará tecnicamente os controles aplicados e o nível de conformidade individual de cada estação de trabalho e servidor, abrangendo:

19.2.2.1. Tratamento de incidentes: ações realizadas para mitigação dos riscos;

19.2.2.2. Relatório forense: Relatório demonstrando as ações do ator de ameaça;

19.2.2.3. Principais riscos: Principais riscos identificados;

19.2.2.4. Plano Diretor: Plano de ação e recomendações para lidar com os riscos residuais;

19.3. A CONTRATADA deverá emitir relatórios técnicos e auxiliar o CRCMG na elaboração de respostas às autoridades competentes, quando necessário e a critério do CRCMG, no caso de eventual incidente de segurança da informação.

20. MODALIDADE DA LICITAÇÃO

Pregão Eletrônico.

21. VALOR DE REFERÊNCIA

21.1. O valor de referência, que corresponde ao **VALOR GLOBAL MÁXIMO** que o CRCMG se propõe a pagar pela prestação dos serviços, objeto deste Termo de Referência, pelo período de 60 (sessenta) meses é de R\$ 872.250,00 (oitocentos e setenta e dois mil duzentos e cinquenta reais).

VALOR DE REFERÊNCIA	
Estimativa Mensal	Estimativa Global 60 meses
R\$ 14.537,50	R\$ 872.250,00

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- 21.2. No valor que vir a oferecer deverão ser incluídas todas as despesas com os profissionais e equipamentos, bem como, taxas, alimentação, transporte, hospedagem, enfim, todos os encargos fiscais, comerciais, trabalhistas e previdenciários, resultantes da prestação dos serviços objeto deste Procedimento.

22. CRITÉRIO DE JULGAMENTO DAS PROPOSTAS

- 22.1. No julgamento das propostas, será considerada vencedora a que apresentar **MENOR PREÇO GLOBAL**, desde que atendidas às especificações constantes deste Edital e de seus Anexos.
- 22.2. Será desclassificada a proposta que, para sua viabilização, apresente vantagens ou subsídios que não estejam previamente autorizados em lei, assim como as que não se encontrem em conformidade com os requisitos estabelecidos no presente Edital.
- 22.3. O julgamento das propostas será de acordo com a sistemática do site de compras denominado www.comprasnet.gov.br, em consonância com a legislação vigente.

23. DO PRAZO DE VIGÊNCIA DO CONTRATO

O contrato vigorará pelo prazo de 60 (sesenta) meses, a contar da data de sua assinatura e será regido pelas Leis nº 10.520/02, nº 8.666/93 e pelo Código Civil Brasileiro.

24. DA GARANTIA CONTRATUAL

- 24.1. A CONTRATADA, no prazo de até 20 (vinte) dias, contado a partir da data de assinatura deste contrato, prestará garantia de cumprimento das obrigações contratuais, correspondente a 5 % (cinco por cento) do valor estimado para a execução dos serviços, objeto deste contrato.
- 24.1.1. O prazo estipulado no subitem anterior poderá ser prorrogado por igual período, a juízo do CRCMG, à vista das justificativas que lhe forem apresentadas pela CONTRATADA.
- 24.1.2. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa, nos termos do item 25.2.4.5.
- 24.1.3. O atraso superior a 30 (trinta) dias corridos, após os prazos previstos nos subitens 24.1 e 24.1.1, autoriza a CONTRATANTE a promover a rescisão deste contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os incisos I e II do art. 78 da Lei nº 8.666/1993, sem prejuízo de outras sanções previstas na Lei e neste contrato.
- 24.2. Caberá à CONTRATADA escolher uma das modalidades previstas no art. 56 da Lei nº 8.666/1993:
- a) caução em dinheiro ou títulos da dívida pública;
 - b) seguro-garantia;
 - c) fiança bancária.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

24.3. Em se tratando de garantia prestada por meio de caução em dinheiro, o depósito deverá ser feito obrigatoriamente na Caixa Econômica Federal, conforme determina o art. 82 do Decreto n.º 93.872/1986, em caderneta de poupança, em favor do CRCMG, e será corrigida pelos índices oficiais aplicados à essa modalidade de depósito bancário.

24.4. Se a opção for pelo seguro-garantia:

a) a apólice indicará o CRCMG como beneficiário, devendo ser emitida por instituição autorizada pela Superintendência de Seguros Privados (SUSEP) a operar no mercado securitário, que não se encontre sob regime de direção fiscal, intervenção, liquidação extrajudicial ou fiscalização especial e que não esteja cumprindo penalidade de suspensão imposta pela autarquia;

b) seu prazo de validade deverá corresponder ao período de vigência deste contrato, acrescido de 90 (noventa) dias para apuração de eventual inadimplemento da CONTRATADA, ocorrido durante a vigência contratual, e para a comunicação da expectativa de sinistro ou do efetivo aviso de sinistro à instituição emitente, observados os prazos prescricionais pertinentes;

c) a apólice deve prever expressamente responsabilidade da seguradora por todas e quaisquer multas de caráter sancionatório aplicadas à CONTRATADA.

24.5. Se a opção for pela fiança bancária, o instrumento de fiança deve:

a) ser emitido por instituição financeira que esteja autorizada pelo Banco Central do Brasil a funcionar no Brasil e que não se encontre em processo de liquidação extrajudicial ou de intervenção da autarquia;

b) ter prazo de validade correspondente ao período de vigência deste contrato, acrescido de 90 (noventa) dias para apuração de eventual inadimplemento da CONTRATADA, ocorrido durante a vigência contratual, e para a comunicação do inadimplemento à instituição financeira, observados os prazos prescricionais pertinentes;

c) ter afirmação expressa do fiador de que, como devedor solidário, fará o pagamento ao CRCMG, independentemente de interpelação judicial, caso o afiançado não cumpra suas obrigações;

d) ter renúncia expressa do fiador ao benefício de ordem e aos direitos previstos nos arts. 827 e 838 do Código Civil Brasileiro.

24.6. Se a opção for pelo título da dívida pública, este deverá:

a) ter sido emitido sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil;

b) ser avaliado por seu valor econômico, conforme definido pelo Ministério da Economia.

24.7. A garantia, qualquer que seja a modalidade escolhida, assegurará o pagamento de:

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- a) prejuízos advindos do não cumprimento do objeto deste contrato e do não adimplemento das demais obrigações nele previstas;
- b) prejuízos causados ao CRCMG ou a terceiro, decorrentes de culpa ou dolo durante a execução deste contrato;
- c) multas moratórias e punitivas aplicadas pelo CRCMG à CONTRATADA; e
- d) obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza, não adimplidas pela CONTRATADA.
- 24.7.1. A modalidade seguro garantia somente será aceita se contemplar todos os eventos indicados no subitem 24.7.
- 24.8. Não serão aceitos seguro-garantia ou fiança bancária que contenham cláusulas contrárias aos interesses do CRCMG.
- 24.9. Sem prejuízo das sanções previstas em lei e neste contrato, a não prestação da garantia exigida implicará sua imediata rescisão.
- 24.10. Se o valor da garantia vier a ser utilizado, total ou parcialmente, no pagamento de qualquer obrigação vinculada a este ajuste, incluída a indenização a terceiros, a CONTRATADA deverá proceder à respectiva reposição, no prazo máximo de 20 (vinte) dias, contados da data do recebimento da notificação do CRCMG.
- 24.11. Se houver acréscimo ao valor deste contrato, a CONTRATADA se obriga a fazer a complementação da garantia no prazo máximo 20 (vinte) dias, contados da data do recebimento da notificação do CRCMG.
- 24.12. Na hipótese de prorrogação deste contrato, o CRCMG exigirá nova garantia, escolhida pela CONTRATADA entre as modalidades previstas na Lei n.º 8.666/1993.
- 24.13. O documento de constituição da nova garantia deverá ser entregue ao CRCMG no prazo máximo de 20 (vinte) dias, contados da data de assinatura do respectivo termo aditivo.
- 24.14. A garantia, ou seu saldo, será liberada ou restituída, a pedido da CONTRATADA, no prazo de 90 (noventa) dias após o término do prazo de vigência deste contrato, mediante certificação, por seu gestor ou fiscal, de que os serviços foram realizados a contento e desde tenham sido cumpridas todas as obrigações aqui assumidas.
- 24.15. A qualquer tempo, mediante entendimento prévio com o CRCMG, poderá ser admitida a substituição da garantia, observadas as modalidades previstas no subitem 24.2 deste contrato.
- 24.15.1. Aceita pelo CRCMG, a substituição da garantia será registrada no processo administrativo por meio de apostilamento.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

25. DAS SANÇÕES ADMINISTRATIVAS

25.1. Comete infração administrativa nos termos da Lei nº 10.520 de 2002 e da Lei nº 8.666/1993, a CONTRATADA que:

- 25.1.1. inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;
- 25.1.2. ensejar o retardamento da execução do objeto;
- 25.1.3. falhar ou fraudar na execução do contrato;
- 25.1.4. comportar-se de modo inidôneo; ou
- 25.1.5. cometer fraude fiscal.

25.2. Pela inexecução total ou parcial do objeto deste contrato ou descumprimento de obrigações, a Administração poderá aplicar à CONTRATADA as seguintes sanções:

- 25.2.1. **Advertência por escrito**, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado;
- 25.2.2. **Suspensão temporária do direito de participar de licitação e impedimento de contratar** com a Administração, pelo prazo de até 2 (dois) anos;
- 25.2.3. **Impedimento de licitar e contratar** com órgãos e entidades da União, com o consequente descredenciamento no SICAF pelo prazo de até 5 (cinco) anos.
- 25.2.4. **Multa de:**
 - 25.2.4.1. 0,5% (cinco décimos por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, limitada a incidência a 15 (quinze) dias. Após o décimo quinto dia e a critério da Administração, no caso de entrega com atraso, poderá ocorrer a não aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença;
 - 25.2.4.2. 10% (dez por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;
 - 25.2.4.3. em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida;
 - 25.2.4.4. 3% (três por cento), 5% (cinco por cento) ou 10% (dez por cento), sobre o valor total da contratação, em caso de descumprimento de obrigações assumidas, por ocorrência, conforme a gradação estabelecida nos subitens e tabela abaixo.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

25.2.4.5. 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso na apresentação da garantia (seja para reforço ou por ocasião de prorrogação), observado o máximo de 2% (dois por cento). O atraso superior a 25 (vinte e cinco) dias autorizará a Administração CONTRATANTE a promover a rescisão do contrato;

25.3. Na aplicação das sanções, o CRCMG levará em consideração a efetiva gravidade da conduta do infrator, o caráter educativo da pena, bem como, o real dano causado ao Conselho. Sendo assim, as multas e outras sanções aplicadas só poderão ser relevadas, motivadamente, por conveniência administrativa.

25.4. As FALTAS LEVES serão puníveis com a aplicação da penalidade de advertência e/ou multa, no percentual de 3% (três por cento), caracterizando-se pelo descumprimento parcial de deveres de pequena monta, assim entendidas como aquelas que não acarretam prejuízos relevantes aos serviços da Administração e a despeito delas, a regular prestação dos serviços não fica inviabilizada.

25.5. As FALTAS MÉDIAS serão puníveis com a aplicação da penalidade de multa no percentual de 5% (cinco por cento), caracterizando-se pela recorrência de quaisquer FALTAS LEVES ou pelo descumprimento parcial ou total de obrigação que acarrete prejuízos aos objetivos da Administração, mas sem inviabilizar total ou parcialmente a execução dos serviços.

25.6. As FALTAS GRAVES serão puníveis com a aplicação das penalidades de multa no percentual de 10% (dez por cento), podendo ser aplicada cumulativamente as sanções de suspensão temporária do direito de participar em licitação e impedimento de contratar com a Administração ou impedimento de licitar e contratar com órgãos e entidades da União, caracterizando-se pela recorrência de quaisquer FALTAS MÉDIAS ou pelo descumprimento parcial ou total de obrigação que acarrete prejuízos relevantes aos objetivos da Administração, inviabilizando a execução da contratação em decorrência de conduta culposa ou dolosa da contratada.

25.7. Afim de nortear na efetiva aplicabilidade das gradações que tratam nos subitens acima, será utilizada a seguinte classificação:

TIPO DE FALTA	GRAVIDADE
Veicular qualquer tipo de publicidade acerca do Contrato, salvo se houver prévia autorização da Administração do Conselho.	LEVE
Abster-se de prestar as informações e esclarecimentos que venham a ser solicitados pelo CRCMG, atendendo às solicitações nos prazos especificados.	LEVE
Não disponibilizar uma conta de e-mail para fins de comunicação entre as partes, bem como, endereço comercial e telefone de contato ou, em caso de alteração, não comunicar prontamente ao CRCMG.	MÉDIA
Alocar, na prestação dos serviços, profissionais com formação e qualificações não adequadas ou incompatíveis com a prestação dos serviços, conforme estabelecido no Termo de Referência.	MÉDIA

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

Utilizar empregado sem qualificação para a execução dos serviços ou, em caso de desligamento, não proceder à pronta substituição por outro profissional com a formação e qualificações estabelecidas no Termo de Referência.	MÉDIA
Provocar, por meio de seus empregados e representantes, qualquer dano patrimonial ou à imagem e reputação do CRCMG.	MÉDIA
Não substituir, após solicitação do CRCMG, empregado que tenha conduta inconveniente ou incompatível com suas atribuições.	MÉDIA
Prestar os serviços sem obedecer estritamente às condições estabelecidas neste Termo de Referência e no Contrato pactuado.	GRAVE
Não cumprir os prazos de entrega e execução dos serviços estipulados neste Termo de Referência.	GRAVE
Não providenciar a imediata correção das deficiências apontadas pelo fiscal do Contrato, quanto à execução contratual.	GRAVE
Deixar de manter todas as condições de habilitação e qualificação que ensejaram sua contratação, durante todo o período de vigência do Contrato.	GRAVE
Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços contratados.	GRAVE

25.7.1. As faltas cometidas pela Contratada que não se enquadrarem em nenhuma das ocorrências previstas na tabela acima, serão avaliadas caso a caso, no âmbito do Processo Administrativo.

25.7.2. Ao longo do período de validade da Ata, de 12 meses, o acúmulo de condutas faltosas cometidas de forma reiterada, de mesma classificação ou não, bem como as reincidências, ensejará a aplicação, pela administração de penalidades relacionadas às faltas de maior gravidade, considerando que, o fato de a Administração relevar qualquer falta, não implicará em novação.

25.8. Reserva-se ao CRCMG o direito de reter e compensar, dos pagamentos da contratada, as multas referidas nos subitens anteriores, assegurado o contraditório e a apresentação de defesa prévia, nos termos da legislação vigente.

25.9. As sanções previstas nos subitens 25.2.1, 25.2.2 e 25.2.3 poderão ser aplicadas à CONTRATADA cumulativamente com as multas previstas no subitem 25.2.4.

25.10. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

25.10.1. tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

25.10.2. tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

25.10.3. demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

25.11. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

25.11.1. As partes concordam que o envio e o recebimento das notificações e comunicações em geral, inclusive no âmbito de processo administrativo que venha a ser instaurado, serão realizados por meio de e-mail.

25.12. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

25.13. As penalidades serão obrigatoriamente registradas no SICAF.

25.14. Além das sanções acima previstas, o contrato poderá ser rescindido pelos motivos previstos nos artigos 77 a 80 da Lei nº 8.666/93.

26. OBRIGAÇÕES DA CONTRATADA

26.1. Prestar os serviços, objeto deste Edital, cumprindo os prazos e atendendo integralmente a todas condições e especificações estabelecidas neste Termo de Referência.

26.2. Entregar os serviços objeto desse Edital, obedecendo aos prazos estipulados neste Termo de Referência.

26.3. Arcar com todos os custos necessários à execução dos serviços, objeto deste procedimento, tais como materiais, softwares e equipamentos, alimentação, transporte, hospedagem, instalações, mão de obra e quaisquer outros que forem pertinentes ao cumprimento do objeto, em conformidade com este Termo de Referência.

26.4. Assumir e cumprir todas as obrigações trabalhistas previstas em legislação e normas específicas, responsabilizando-se, exclusivamente, pela remuneração, encargos sociais e previdenciários, benefícios e demais despesas referentes a seus profissionais, tendo em vista que não será estabelecido nenhum vínculo empregatício ou de responsabilidade entre os profissionais disponibilizados para a execução dos serviços contratados e o CRCMG.

26.5. Responsabilizar-se pela idoneidade e pelo comportamento de seus empregados, prepostos ou subordinados.

26.6. Utilizar, na execução dos serviços, somente profissionais especializados e, em caso de desligamento, promover a reposição do profissional por outro com a mesma formação e qualificações estabelecidas neste Termo de Referência.

26.7. Reparar, corrigir, remover ou substituir às suas expensas, no total ou em parte, o objeto deste procedimento em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

materiais empregados, no prazo de 48 (quarenta e oito) horas da notificação, sem ônus par ao CRCMG.

- 26.8. Prestar todos os esclarecimentos que forem solicitados pelo CRCMG, atendendo de imediato às solicitações de seus representantes.
- 26.9. Informar, de imediato, as alterações de endereço, de número de telefones e de e-mails.
- 26.10. Assumir inteira responsabilidade, civil, administrativa e penal por danos materiais ou pessoais causados ao CRCMG e/ou a terceiros provocados por ineficiência ou irregularidades cometidas por seus empregados, contratados ou prepostos envolvidos na execução do contrato, decorrentes de dolo ou culpa.
- 26.11. Guardar o mais absoluto sigilo em relação às informações ou documentos de qualquer natureza a que venham tomar conhecimento, respondendo, administrativa, civil e criminalmente por sua indevida divulgação e/ou incorreta ou descuidada utilização.
- 26.11.1. A CONTRATA deverá apresentar, o momento de assinatura do contrato, Termo de Confidencialidade e Sigilo do Prestador, constante do Anexo VIII do Edital.
- 26.12. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, observando a prática da boa técnica e a legislação vigente.
- 26.13. Emitir as notas fiscais com as devidas deduções legais, devendo ser apresentada, juntamente, com as certidões de regularidade junto ao FGTS, ao INSS e à Justiça do Trabalho, além da Declaração de Optante pelo Simples Nacional, se for o caso.
- 26.14. Manter, durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas neste Edital.
- 26.15. Aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até 25% (vinte e cinco por cento) do valor inicial do contrato, na forma da legislação vigente.
- 26.16. Submeter-se à fiscalização do CRCMG, na execução dos serviços, seguindo todas as orientações repassadas.

27. OBRIGAÇÕES DO CRCMG

- 27.1. Proporcionar as condições necessárias à execução dos serviços ora contratados, assim como prestar, prontamente, as informações e os esclarecimentos que venham a ser solicitados pela contratada;
- 27.2. Efetuar o pagamento à contratada, de acordo com as condições de preço e prazo estabelecidas no contrato.



Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

27.3. Acompanhar e fiscalizar o andamento dos serviços, por intermédio do funcionário do CRCMG designado como Fiscal do Contrato.

27.4. Rejeitar, no todo ou em parte, os serviços entregues em desacordo com as obrigações assumidas pela empresa contratada.

27.5. Comunicar a contratada toda e qualquer ocorrência relacionada com a execução do serviço.

27.6. Notificar a contratada, por escrito e com antecedência, sobre multas, penalidades e quaisquer débitos de sua responsabilidade.

28. SUBCONTRATAÇÃO

Não será admitida a subcontratação do objeto licitatório.

29. ALTERAÇÃO SUBJETIVA

28.1. É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa do Contratante à continuidade do contrato.

30. RESPONSÁVEIS PELO TERMO DE REFERÊNCIA

O presente Termo de Referência foi elaborado pela Gerência de Tecnologia da Informação e pela Gerência Administrativa e Financeira (GEADF) em consonância com as disposições legais e normativas aplicáveis e com o interesse e a conveniência da Administração, sendo objeto de exame e aprovação do Ordenador de Despesa do Conselho, e passará a integrar o processo administrativo formalizado visando à instauração do certame licitatório e a efetividade da contratação.

DATA

ASSINATURA DO GERENTE DE TECNOLOGIA DA INFORMAÇÃO

Janeiro/2023

DATA

ASSINATURA DO GERENTE ADMINISTRATIVO E FINANCEIRO

Janeiro/2023

DATA

ASSINATURA DO PRESIDENTE DO CRCMG

Janeiro/2023

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

ANEXO II – MODELO DE PROPOSTA

Ao
CONSELHO REGIONAL DE CONTABILIDADE DE MINAS GERAIS

PREGÃO ELETRÔNICO Nº 001/2023

EMPRESA: _____

CNPJ: _____

ENDEREÇO: _____

TELEFONE: _____

(E-MAIL): _____

Em atendimento ao Edital do Pregão em epígrafe, apresentamos a(s) seguinte(s) proposta(s) de preços.

ITEM I	
OBJETO: CONTRATAÇÃO DE EMPRESA ESPECIALIZADA EM SERVIÇOS GERENCIADOS DE SEGURANÇA, INCLUINDO:	
1. Serviços de monitoramento de ataques cibernéticos e resposta a incidentes: 1.1. Visa o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados à CONTRATANTE, através de fornecimento de solução de correlacionamento de logs de aplicações, serviços e infraestrutura do CONTRATANTE, que possam gerar eventos de segurança da informação, aos quais devem ser analisados, remediados, contidos e documentados, podendo estes serem transformados em um incidente de segurança da informação, obedecendo um processo cíclico e rigoroso de gestão de eventos.	
2. Serviços de Gestão de Vulnerabilidades: 2.1. Visando, de forma proativa e recorrente, identificar possíveis vulnerabilidades de segurança da informação na infraestrutura, nas aplicações e nas contas de usuários do CONTRATANTE, a fim de evitar que ataques cibernéticos direcionados à CONTRATANTE obtenha sucesso, explorando tais vulnerabilidades já conhecidas.	
3. Serviço de monitoramento, detecção e resposta a incidentes para Endpoints. 3.1. Visando à proteção, monitoramento contínuo e operação de solução dedicada a proteção de estações e servidores do CONTRATANTE, realizando de forma proativa o bloqueio de códigos maliciosos tipo vírus, Malware - blindando os ativos protegidos também contra Ransomware, oferecendo possibilidade de realização de "Rollback" de arquivos alvos de códigos maliciosos, oferecendo ainda suporte à investigação de ataques através da trilha de registros de eventos forense.	
Os serviços serão prestados em total conformidade com as condições, detalhamento e especificações constantes do Termo de Referência Anexo I do Edital nº 001/2023.	
VALOR MENSAL	R\$ (.....)
VALOR GLOBAL PERÍODO DE 60 (SESSENTA MESES)	R\$ (.....)

119

Rua Cláudio Manoel, 639 - Savassi – Belo Horizonte/MG – Cep: 30140-105
 Telefone: (31) 3269-8400 - www.crcmg.org.br



Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

Validade da Proposta: 60 (sessenta) dias.

Condições de pagamento: O CRCMG efetuará o pagamento em até 10 (dez) dias úteis, após a prestação dos serviços, mediante apresentação da nota fiscal, com as devidas deduções legais, bem como das certidões de regularidade junto ao FGTS, ao INSS e à Justiça do Trabalho, além da Declaração de Optante pelo Simples Nacional, se for o caso.

Serão descontados sobre os pagamentos a serem realizados, as devidas retenções de tributos e contribuições, conforme determina a Instrução Normativa nº. 1.234, de 11/01/2012, da Secretaria da Receita Federal.

Submetemo-nos a todas as condições do Edital nº 001/2023, inclusive quanto ao cumprimento na íntegra do respectivo Termo de Referência - Anexo I.

Dados do representante legal da empresa, responsável pela assinatura do Contrato:

Nome:

Função:

CPF:

Telefone/Fax:

Endereço Eletrônico (e-mail):

_____ de _____ de 2023.

Assinatura do representante legal da empresa

Rua Cláudio Manoel, 639 - Savassi – Belo Horizonte/MG – Cep: 30140-105
Telefone: (31) 3269-8400 - www.crcmg.org.br

120

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

ANEXO III - MINUTA DE CONTRATO

Contrato de prestação de serviços que entre si fazem, de um lado, o **CONSELHO REGIONAL DE CONTABILIDADE DE MINAS GERAIS**, com sede em Belo Horizonte, Minas Gerais, na Rua Cláudio Manoel, 639, Bairro Savassi, inscrito no CNPJ/MF sob o número 17.188.574/0001-38, representado por seu presidente, Contador XXXXXXXXXXXX, de ora em diante denominado CRCMG, e, de outro, XXXXXXXXXXXX, com sede em XXXXXXXXXXXX, XXXXXXXXXXXX, na Rua/AVXXXXXXXX, nº XXXX, Bairro XXXX, inscrita no CNPJ sob o nº XXXXXX, neste ato representado por seu representante legal, XXXXXXXX, de ora em diante denominada CONTRATADA, sujeitando as partes contratantes às normas constantes na Lei nº 10.520, de 17/7/2002, Lei nº 13.709, de 14/8/2018, Lei Complementar nº 123, de 13/12/2006 e Decreto nº 8.538, de 06/10/2015, com aplicação subsidiária das normas da Lei nº 8.666, de 21/06/93, mediante as cláusulas e condições que se seguem:

CLÁUSULA PRIMEIRA - DO OBJETO

1. Contratação de empresa especializada na prestação de SERVIÇOS GERENCIADOS DE SEGURANÇA, conforme condições e especificações estabelecidas no Anexo I – Termo de Referência deste Edital, conforme condições e especificações estabelecidas no Edital nº 001/2023 e seu Anexo I – Termo de Referência.

CLÁUSULA SEGUNDA - OBRIGAÇÕES DA CONTRATADA E DO CRCMG

2.1. As obrigações da CONTRATADA e do CRCMG são aquelas previstas no Termo de Referência, Anexo I do Edital Pregão Eletrônico nº 001/2023.

CLÁUSULA TERCEIRA - DOS PREÇOS

3.1. Pela execução dos serviços objeto deste contrato o CRCMG pagará a CONTRATADA o valor mensal de R\$ (.....), cujo desembolso dar-se-á com recursos previstos em dotação orçamentária própria, sob a rubrica 6.3.1.3.02.01.005, observado o item 4.1 deste contrato.

3.2. O valor global pela prestação dos serviços no período de 60 (sessenta) meses é de R\$ (.....), observado o item 4.1 deste contrato.

3.3. Serão descontados sobre os pagamentos a serem realizados, as devidas retenções de tributos e contribuições, conforme determina a Instrução Normativa nº. 1.234, de 11/01/2012, da Secretaria da Receita Federal.

3.4. Os preços são fixos e irredutíveis no prazo de um ano contado da data limite para a apresentação das propostas.

3.4.1. Dentro do prazo de vigência do contrato e mediante solicitação da contratada, os preços contratados poderão sofrer reajuste após o interregno de um ano, aplicando-se o índice IPCA, acumulado nos 12 (doze) meses anteriores a data base ou outro índice que venha a substituí-lo, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

3.4.2. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

CLÁUSULA QUARTA - DAS CONDIÇÕES DE PAGAMENTO

4.1. Os pagamentos terão início somente após a instalação da solução e a completa disponibilização dos serviços, mediante o aceite definitivo da CONTRATANTE.

4.1.1. O CRCMG efetuará o pagamento em até 10 (dez) dias úteis, contados a partir do recebimento da Nota Fiscal com as devidas deduções legais.

4.1.2. Considera-se ocorrido o recebimento da nota fiscal ou fatura no momento em que o órgão contratante atestar a execução do objeto do contrato.

4.1.3. A Nota Fiscal deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da Lei nº 8.666, de 1993.

4.2. Serão descontados sobre o pagamento a ser realizado, as devidas retenções de tributos e contribuições, conforme determina a Instrução Normativa nº. 1.234, de 11/01/2012, da Secretaria da Receita Federal.

4.3. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante;

4.4. Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

4.5. Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante.

4.6. Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018.

4.7. Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

4.8. Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

4.9. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.

4.10. Será rescindido o contrato em execução com a contratada inadimplente no SICAF, salvo por motivo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante.

4.11. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

$EM = I \times N \times VP$, sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

$$I = (TX) \quad I = \frac{(6 / 100)}{365}$$

$$TX = \text{Percentual da taxa anual} = 6\% \\ I = 0,00016438$$

CLÁUSULA QUINTA - DA VIGÊNCIA

5.1. O presente contrato vigorará pelo prazo de 60 (sessenta) meses, a contar da data de sua assinatura e será regido pelas Leis nº 10.520/2002, nº 8.666/93 e pelo Código Civil Brasileiro.

CLÁUSULA SEXTA - DO ACOMPANHAMENTO E FISCALIZAÇÃO

6.1. O contrato será acompanhado e fiscalizado conforme critérios e condições estabelecidos no Termo de Referência – Anexo I do Edital Pregão Eletrônico nº 001/2023, observadas as designações específicas.

CLÁUSULA SÉTIMA - DAS SANÇÕES

7.1. As sanções relacionadas à execução do contrato são aquelas previstas no Termo de Referência, Anexo I do Edital Pregão Eletrônico nº 001/2023.

CLÁUSULA OITAVA - DA RESCISÃO

8.1. O contrato poderá ser rescindido pelos motivos previstos nos artigos 77 a 80 da Lei nº 8.666/93.

CLÁUSULA NONA - DA CONFORMIDADE COM A LEI GERAL DE PROTEÇÃO DE DADOS

9.1. A Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, (LGPD), é a legislação brasileira que regula as atividades de tratamento de dados pessoais. O CRCMG seguindo as boas práticas de governança e *compliance* está comprometido com seus deveres de garantia da privacidade e de proteção de dados pessoais, e preza em todas as relações contratuais que os envolvidos adotem boas práticas de governança, visando sempre o interesse do respeito a legislação vigente.

9.2. Neste sentido, a CONTRATADA declara estar ciente que a CONTRATANTE é uma entidade de fiscalização tendo como uma de suas atividades precípuas, o registro de categoria profissional, regida pelo princípio do acesso à informação normatizado pela Lei 12.527/2011 (Lei de Acesso à Informação). Sendo assim, realiza o tratamento

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

de dados para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais e cumprir as atribuições legais do serviço público, e, portanto, eventuais dados pessoais dos sócios, representantes legais, prepostos e demais envolvidos na relação do objeto do presente contrato, estarão disponíveis no Portal da Transparência, nos termos do art. 23 da LGPD.

9.3. A CONTRATADA no ato da assinatura do presente instrumento, declara que se encontra adequada e capaz de garantir a devida proteção e manuseio dos dados pessoais que sejam tangíveis, ou que, pessoalmente identifiquem ou tornem identificáveis, quaisquer empregados, clientes, agentes, usuários final, fornecedor, contatos, ou qualquer pessoa natural cujos dados pessoais sejam objeto de tratamento das respectivas instituições a quem pertencem os sócios quotistas incluindo suas filiais, subsidiárias, ou grupo econômico a que pertençam, em conformidade com a LGPD.

9.4. O tratamento de dados pessoais dar-se-á de acordo com as bases legais previstas nas hipóteses dos arts. 7º e/ou 11 da Lei 13.709/2018 às quais se submeterão os serviços, e para propósitos legítimos, específicos, explícitos e informados ao titular.

9.5. As partes deverão adotar todas as políticas e medidas protetivas definitivas na LGPD, promovendo políticas de proteção de dados com adoção de ferramentas tecnológicas, jurídicas e humanas, para coleta e proteção de dados pessoais de pessoas naturais, no âmbito do desenvolvimento do objeto do presente contrato.

9.6. Ressalvado o disposto no item 9.7, é vedada à CONTRATADA a subcontratação do processamento dos dados pessoais recebidos, bem como a transferência do processamento ou tratamento para qualquer empresa ou terceiro, inclusive no exterior, sem o consentimento prévio por escrito do CONTRATANTE, no âmbito do objeto deste contrato.

9.7. A CONTRATADA, no âmbito de suas relações comerciais próprias, poderá contratar serviços de armazenamento em nuvem para os dados relacionados ao presente contrato, desde que essenciais à execução dos serviços e em acordo com as finalidades e os limites deste ajuste e as disposições da Lei n.º 13.709/2018 (LGPD).

9.7.1. A CONTRATADA atesta que a prestadora dos serviços de armazenamento em nuvem possui condições de fornecer o nível adequado de proteção dos dados sob a sua guarda, em conformidade com as exigências estipuladas na Lei n.º 13.709/2018 (LGPD).

9.7.2. A prestadora dos serviços de armazenamento em nuvem atuará na condição de suboperadora dos dados e, no caso de descumprir as determinações da Lei n.º 13.709/2018 (LGPD), responderá a CONTRATADA perante o CRCMG.

9.8. A CONTRATADA se compromete a, na execução das suas atividades contratualmente previstas, não coletar dados pessoais de terceiros sem a observância dos pressupostos da LGPD, tampouco compartilhar ou enviar tais dados para a CONTRATANTE, quando seu tratamento estiver em desconformidade com a referida legislação, sob pena de caracterizar inadimplemento contratual, passível, inclusive, de motivar a rescisão prevista no presente instrumento.

9.9. Os dados obtidos em razão desse contrato serão armazenados em um banco de dados seguro, com garantia de registro das transações realizadas na aplicação de acesso (log) e adequado controle de acesso baseado em

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

função (*role based access control*) e com transparente identificação do perfil dos credenciados, tudo estabelecido como forma de garantir inclusive a rastreabilidade de cada transação e a franca apuração, a qualquer momento, de desvios e falhas, vedado o compartilhamento desses dados com terceiros;

9.10. A CONTRATADA se compromete com a qualidade dos dados pessoais eventualmente fornecidos à CONTRATANTE em decorrência do presente contrato, zelando pela entrega de dados corretos e atualizados, buscando sempre o melhor interesse dos titulares, respeitando os seus direitos e reforçando sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, nos termos do artigo 23 da LGPD.

9.11. Encerrada a vigência do contrato ou não havendo mais necessidade de utilização dos dados pessoais, sejam eles sensíveis ou não, a CONTRATADA interromperá o tratamento dos dados pessoais, e os eliminará completamente com todas as cópias porventura existentes (seja em formato digital ou físico), no prazo máximo de 30 (trinta) dias, salvo quando a CONTRATADA tenha que mantê-los para cumprimento de obrigação legal ou outra hipótese da LGPD, sob pena de responsabilização administrativa, cível e penal.

9.12. Em caso de eventual coleta de dados pessoais sensível, esta será realizada mediante prévia aprovação do CONTRATANTE, responsabilizando-se a CONTRATADA por obter o consentimento dos titulares (salvo nos casos em que opere outra hipótese legal de tratamento). Os dados assim coletados só poderão ser utilizados na execução dos serviços especificados neste contrato, e em hipótese alguma poderão ser compartilhados ou utilizados para outros fins.

9.13. Eventualmente, as partes podem ajustar que o CONTRATANTE será responsável por obter o consentimento dos titulares, observadas as demais condicionantes no item 9.11 acima.

9.14. As partes informarão imediatamente entre si caso o titular dos dados, a Autoridade Nacional de Proteção de Dados (ANPD) ou terceiros solicitem informações sobre o tratamento de dados pessoais relacionados ao presente contrato ou mesmo determine, legalmente amparada, a eliminação ou anonimização dos dados compartilhados.

9.15. A CONTRATADA cooperará com o CONTRATANTE no cumprimento das obrigações referentes ao exercício dos direitos dos titulares previstos na LGPD e nas Leis e Regulamentos de Proteção de Dados em vigor e, também, no atendimento de requisições e determinações do Poder Judiciário, Ministério Público e órgãos de controle externo.

10. CLÁUSULA DÉCIMA - DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO CRCMG

10.1. A CONTRATADA deverá tomar conhecimento da Política de Segurança da Informação do CRCMG, instituída pela Resolução CRCMG nº 441/2021, disponível em <http://cadastro.crcmg.org.br/ged/>, e se comprometer com a observância e o acatamento de suas diretrizes, sempre que tiver acesso a qualquer informação ou comunicação do CRCMG, oriundas da relação firmada por este instrumento.

CLÁUSULA DÉCIMA PRIMEIRA – DA ASSINATURA ELETRÔNICA/DIGITAL

11.1. Nos termos da Lei nº 14.063/2020 e do Decreto nº 10.543/2020, as partes e as testemunhas concordam expressamente em utilizar assinatura eletrônica para ratificação e legitimação dos termos ajustados no presente instrumento, reconhecendo que a formalização, por esse procedimento, é bastante suficiente à sua integral validade jurídica e vinculação das partes ao Contrato.



Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

11.2. As partes renunciam à possibilidade de exigir a troca, envio ou entrega das vias originais (não eletrônicas) assinadas do instrumento, bem como renunciam ao direito de recusar ou contestar a validade das assinaturas digitais ou eletrônicas, na medida máxima permitida pela legislação aplicável.

CLÁUSULA DÉCIMA SEGUNDA - DO FORO

12.1. Fica eleito o foro da Justiça Federal - Subseção de Belo Horizonte, para dirimir as questões oriundas deste contrato, com renúncia de qualquer outro por mais privilegiado que seja.

E por estarem as partes justas e contratadas, assinam o presente instrumento em 02 (duas) vias de igual teor, para um só efeito.

Considera-se o contrato celebrado na data em que o último representante legal das partes, neste instrumento, assinou.

Belo Horizonte,

CONSELHO REGIONAL DE CONTABILIDADE DE MINAS GERAIS
Contador XXXXXXXX

EMPRESA XXXX
XXXXXXXXX – XXXXXXXX

Testemunhas

Assinatura:

Assinatura:

CPF:

CPF:

Rua Cláudio Manoel, 639 - Savassi – Belo Horizonte/MG – Cep: 30140-105
Telefone: (31) 3269-8400 - www.crcmg.org.br

126

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

ANEXO IV - CATÁLOGO DE SERVIÇO

Serviço de monitoramento de ataques cibernéticos e resposta a incidentes		
Item	Descrição	Prioridade
Customização de Regras	Customização de 2 (dois) casos de uso por ano	P7
Criação de Conectores	Criação de 1 (um) conector por ano	P8
Monitoramento de Ataques Cibernéticos	Eventos de Informação	P4
	Eventos de Aviso	P3
	Eventos de Exceção	P2
Resposta a Incidentes de Segurança	Apoio a Resposta de Incidente Crítico - Sistema totalmente inoperante com impacto nas operações críticas de negócio	P1
	Apoio à Resposta de Incidente Alto - Sistema parcialmente inoperante com impacto nas operações críticas de negócio	P2
	Apoio à Resposta de Incidente Médio - Sistema parcialmente inoperante sem impacto nas operações críticas de negócio	P3
	Apoio à Resposta de Incidente Baixo - Informacional, ajustes na configuração, dúvidas e/ou esclarecimentos	P4
Plano de Resposta a Incidentes	Apoio na Elaboração do Plano de Resposta	P7

Tabela 2- Serviços de monitoramento de ataques cibernéticos e resposta a incidentes

Serviço de Gestão de Vulnerabilidades		
Item	Descrição	Prioridade
Varreduras de vulnerabilidade	Checação (Scan) e varredura Diária	P4
	Checação (Scan) e varredura Semanal	P7
	Checação (Scan) e varredura Mensal	P8
Elaboração de Relatórios	Report Executivo Mensal de vulnerabilidades com base em Vetores de Ataque	P8
	Reports automatizados e SMS para cada Scanner Executado	P4
	Report Mensal de ações executadas no processo de gestão de vulnerabilidades	P8
Reuniões	Reunião Mensal de Apresentação dos Reports	P8
	Reunião Mensal de Priorização de ativos e reavaliação da estrutura	P8

Tabela 3- Serviço de Gestão de Vulnerabilidades

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

Serviço de monitoramento, detecção e resposta a incidentes para Endpoints		
Item	Descrição	Prioridade
Operação Reativa	Heath Check - Padronizado	P7
	Relatório de Resumo Mensal de Serviços	P8
Operação Proativa	Notificação de Vulnerabilidades em aplicações e S.O.s	P4
	Reuniões periódicas com proposta de melhoria e evolução da maturidade	P8
	Relatórios customizados	P8
Customização	Criação, Alteração ou Remoção de política de segurança específica	P5
Consulta Informacional	Requisição de suporte para sanar dúvidas	P6
Ativação	Requisição de suporte para ativação de agente	P6
Suspeita de Ameaça	Requisição de suporte para análise de suspeita de anomalia	P5
Impacto no Ambiente	Requisição de suporte para correção de impacto	P4
Parada do Ambiente	Requisição de suporte para restauração do ambiente	P3

Tabela 4- Serviço de monitoramento, detecção e resposta a incidentes para Endpoints



Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

ANEXO V – ATESTADO DE VISTORIA

Atestamos que a empresa xxxxxxxxxxxxxxxxxxxx, inscrita no CNPJ sob nº xxxxxxxxxxxxxxxxxxxx, representada pelo(a) Sr(a). xxxxxxxxxxxxxxxxxxxx, portador(a) do CPF nº xxxxxxxxxxxxxxxxxxxx e RG nº xxxxxxxxxxxxxxxxxxxx, visando à formalização de proposta relativa ao Pregão Eletrônico nº 001/2023, cujo objeto é a contratação de empresa especializada em SERVIÇOS GERENCIADOS DE SEGURANÇA, **REALIZOU VISTORIA** na sede do Conselho Regional de Contabilidade de Minas Gerais (CRCMG), localizada na rua Cláudio Manoel, nº 639, bairro Savassi, Belo Horizonte-MG, local onde os serviços serão prestados, tomando conhecimento das condições, das especificações, da estrutura local, assim como das demais peculiaridades e especificidades inerentes à execução do serviços objeto da contratação, assumindo, dessa forma, todos os riscos e consequências relativos à prestação integral dos serviços, isentando o CRCMG de qualquer ônus futuro por incompatibilidade dos seus custos decorrentes do adimplemento do objeto.

O representante da empresa, para comprovação de sua condição, deverá apresentar:

- Documento de identificação;
- Carta de apresentação devidamente assinada por quem de direito.

Belo Horizonte, XX de XXXX de 2023.

Representante do CRCMG

Recebido:

Rua Cláudio Manoel, 639 - Savassi – Belo Horizonte/MG – Cep: 30140-105
Telefone: (31) 3269-8400 - www.crcmg.org.br

129



Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

ANEXO VI – DECLARAÇÃO DE CIÊNCIA DAS INFORMAÇÕES E CONDIÇÕES DE EXECUÇÃO DOS SERVIÇOS

[EM PAPEL TIMBRADO DA EMPRESA]

A empresa [NOME DA EMPRESA], com sede no endereço: [ENDEREÇO DA EMPRESA], inscrita no CNPJ sob o nº [CNPJ DA EMPRESA], por meio de seu representante legal, Sr(a) [NOME DO REPRESENTANTE DA EMPRESA], portador do CPF nº [CPF DO REPRESENTANTE DA EMPRESA], e RG nº [RG DO REPRESENTANTE DA EMPRESA], para fins de participação no Pregão Eletrônico nº 001/2023, cujo objeto é a contratação de empresa especializada em SERVIÇOS GERENCIADOS DE SEGURANÇA, a serem executados na sede do CRCMG, localizada na rua Cláudio Manoel, nº 639, bairro Savassi, Belo Horizonte-MG, durante o período de 12 (doze) meses, **DECLARA** ter pleno conhecimento das condições, das especificações, da estrutura local, assim como das demais peculiaridades e especificidades inerentes à execução dos serviços objeto da contratação, assumindo, dessa forma, todos os riscos e consequências relativos à prestação integral dos serviços, isentando o CRCMG de qualquer ônus futuro por incompatibilidade dos seus custos decorrentes do adimplemento do objeto.

Belo Horizonte, ____ de _____ de 2023.

Assinatura do representante da empresa

Rua Cláudio Manoel, 639 - Savassi – Belo Horizonte/MG – Cep: 30140-105
Telefone: (31) 3269-8400 - www.crcmg.org.br

130

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

ANEXO VII - DECLARAÇÃO FORMAL DE DISPONIBILIDADE TÉCNICA
QUALIFICAÇÃO TÉCNICA DOS PROFISSIONAIS DA EMPRESA

Eu, [NOME DA PESSOA], pessoa física com residência em [ENDEREÇO DA PESSOA], inscrita no CPF com o n.º [N.º DO CPF], [E-MAIL], atesto, na condição de seu representante, que a empresa [NOME DA EMPRESA], [ENDEREÇO DA EMPRESA], [CNPJ DA EMPRESA], possui, em seus quadros, profissionais com as qualificações técnicas, em conformidade com os requisitos estabelecidos no Termo de Referência do Edital 001/2023, atendendo, no mínimo, as seguintes características relativas à formação acadêmica, certificações e experiências:

1. Qualificações técnicas do **GERENTE DE PROJETO**:

Certificações	Descrição
Ao menos uma das certificações de segurança da informação: • Project Management Professional (PMP); • Prince2 Practitioner Certificate in Project Management; • Professional Scrum Master I;	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em gerência de projetos, com experiência mínima de 12 (doze) anos.

Tabela 1 - Qualificações Gerente de Projeto

2. Qualificações técnicas **PREPOSTO**:

Certificações	Descrição
Ao menos uma das certificações de segurança da informação: • CISSP (Certified Information Systems Security Professional); • CISM (Certified Information Security Manager); • CIA (Certified Intrusion Analyst); • GSEC (GIAC Security Essentials); • GCIH (GIAC Incident Handler); • GMON (GIAC Continuous Monitoring);	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência mínima de 5 (cinco) anos em coordenação e gestão de contratos de serviços continuados.

Tabela 2 - Qualificações do Preposto

3. Qualificações técnicas do(s) **analista(s)** que participará do **GRUPO DE ATAQUE CIBERNÉTICO CONTROLADO (Red Team)**:

Certificações	Descrição
• CompTIA Security+ • CompTIA CySA+	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

e/ou Certified Ethical Hacker Certificação em pelo menos uma das soluções escolhidas para atender o tópico SOBRE AS FERRAMENTAS A SEREM UTILIZADAS	graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.

Tabela 3 - Qualificações Grupo de Ataque Cibernético Controlado (Red Team)

4. As qualificações técnicas do(s) **analista(s)** que participará do **GRUPO DE MONITORAMENTO DE ATAQUES**:

Certificações	Descrição
- CompTIA Security+ e/ou - CompTIA CySA+ e/ou - Certified Ethical Hacker	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de SIEM e ATD. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.

Tabela 4 - Qualificações Grupo de Monitoramento de Ataques

5. As qualificações técnicas do(s) **analista(s)** que participará do **GRUPO DE RESPOSTA A INCIDENTE DE SEGURANÇA (CSIRT – Blue Team)**:

Certificações	Descrição
- CompTIA Security+ - CompTIA CySA+ - Certified Ethical Hacker - CompTIA Pentest+ ou - Computer Hacking Forensic Investigator	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC);

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

	Especializações na área de segurança da informação. Conhecimento avançado em segurança da informação, com experiência em resposta a incidente de segurança da informação. Experiência comprovada de no mínimo 5 (cinco) anos em segurança da informação.

Tabela 5 - Qualificações Grupo de Resposta a Incidente de Segurança (CSIRT – Blue Team)

Observações:

As certificações e os conhecimentos e experiências dos profissionais deverão atender aos requisitos mínimos estabelecidos no Termo de Referência, conforme modelo de declaração constante deste Anexo, para cada profissional, de acordo com sua área de atuação, sob pena de desclassificação da licitante.

No momento da assinatura do contrato, a empresa deverá comprovar o vínculo com os referidos profissionais, apresentando cópia da Carteira de Trabalho e Previdência Social (CTPS), no caso de haver relação de emprego, ou de contrato de prestação de serviços, regidos pela legislação civil.

Em todo caso, os profissionais deverão estar disponíveis à prestação dos serviços de modo permanente, durante toda a vigência contratual.

Não serão aceitos vínculos de natureza eventual ou precária, inclusive os decorrentes de terceirização ou subcontratação.

Belo Horizonte, ____ de _____ de 2023.

Assinatura do representante da empresa



Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

ANEXO VIII - MODELO DE TERMO DE CONFIDENCIALIDADE E SIGILO DO PRESTADOR

A CONTRATADA deverá assinar termo de sigilo e confidencialidade conforme modelo abaixo:

TERMO DE CONFIDENCIALIDADE E SIGILO DO PRESTADOR

Eu, [NOME DA PESSOA], pessoa física com residência em [ENDEREÇO DA PESSOA], inscrita no CPF com o n.º [N.º DO CPF], [E-MAIL], atesto, na condição de seu representante, que a empresa [NOME DA EMPRESA], [ENDEREÇO DA EMPRESA], [CNPJ DA EMPRESA], doravante denominado simplesmente signatário, por tomar conhecimento de informações sobre o ambiente computacional do Conselho Regional de Contabilidade de Minas Gerais, aceita as regras, condições e obrigações seguintes:

1. A não utilizar QUAISQUER informações (Técnicas Administrativas ou Gerenciais), confidenciais ou não, a que tiver acesso, para gerar benefício próprio exclusivo e/ou unilateral, presente ou futuro, ou para o uso de terceiros;
2. A não efetuar nenhuma gravação ou cópia da documentação a que tiver acesso;
3. A não apropriar para mim ou para outrem de QUALQUER material técnico, gerencial ou administrativo que venha a ser disponível;
4. A não repassar o conhecimento das informações, responsabilizando-se por todas as pessoas que vierem a ter acesso às informações, por seu intermédio, e obrigando-se, assim, a ressarcir a ocorrência de qualquer dano e/ou prejuízo oriundo de uma eventual quebra de sigilo ou confidencialidade de todas as informações fornecidas;
5. Em cuidar para que as informações confidenciais fiquem restritas ao conhecimento tão somente das pessoas que estejam diretamente envolvidas nas discussões, análises, reuniões e negócios, devendo cientificá-las da existência deste Termo e da natureza confidencial destas informações.

Neste Termo, as seguintes expressões serão assim definidas:

Informação Confidencial significará toda informação revelada por meio do manual de serviço, excetuando-se deste os níveis permitidos pelo fabricante para os quais o CRCMG tenha sido treinado.

Informação inclui, mas não se limita, à informação relativa às documentações técnicas, relatórios técnicos, operações, instalações, equipamentos, segredos de negócio, segredo de fábrica, dados, habilidades especializadas, projetos, métodos e metodologia, sistemas, softwares, bases de dados, fluxogramas, especializações, componentes, fórmulas, produtos, amostras, diagramas, desenhos de esquema industrial, patentes, oportunidades de mercado e questões relativas a negócios revelados nos manuais de serviço. Não constituirá "Informação" ou "Informação Confidencial" para os propósitos deste Termo aquela que:

- a) Seja de domínio público no momento da revelação ou após a revelação, exceto se isso ocorrer em decorrência de ato ou omissão da Parte Receptora;
- b) Já esteja em poder da Parte Receptora, como resultado de sua própria pesquisa, contanto que a Parte Receptora possa comprovar esse fato;



Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

- c) Tenha sido legitimamente recebida de terceiros;
- d) Seja revelada em razão de uma ordem válida ou de uma ordem judicial, somente até a extensão de tais ordens, contanto que a Parte Receptora tenha notificado a existência de tal ordem, previamente e por escrito, à Parte Reveladora, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis;
- e) Tenham sido objeto de treinamento dos profissionais do CRCMG.

A vigência da obrigação de confidencialidade e sigilo, assumida pela minha pessoa por meio deste termo, terá a validade enquanto a informação não for tornada de conhecimento público por qualquer outra pessoa, ou mediante autorização escrita, concedida à minha pessoa pelas partes interessadas neste termo. Pelo não cumprimento do presente Termo de Confidencialidade e Sigilo, fica o abaixo assinado ciente de todas as sanções judiciais que poderão advir.

Belo Horizonte, ____ de _____ de 2023.

Assinatura do representante da empresa
(Mesmo signatário do contrato)



MANIFESTO DE ASSINATURAS



Código de validação: CWBZR-P4J8L-M58Q4-YUNZY

Esse documento foi assinado pelos seguintes signatários nas datas indicadas (Fuso horário de Brasília):

- ✓ SUELY MARIA MARQUES DE OLIVEIRA (CPF 686.588.426-49) em 23/01/2023 16:53 - Assinado com certificado digital ICP-Brasil

Para verificar as assinaturas, acesse o link direto de validação deste documento:

<https://assinador.crcmg.org.br/validate/CWBZR-P4J8L-M58Q4-YUNZY>

Ou acesse a consulta de documentos assinados disponível no link abaixo e informe o código de validação:

<https://assinador.crcmg.org.br/validate>

Pregão/Concorrência Eletrônica

925152.12023 .10551 .4506 .4944980400



Conselho Regional de Contabilidade de Minas Gerais

Ata de Realização do Pregão Eletrônico

Nº 00001/2023

Às 09:40 horas do dia 06 de fevereiro de 2023, reuniram-se o Pregoeiro Oficial deste Órgão e respectivos membros da Equipe de Apoio, designados pelo instrumento legal PORTARIA CRCMG 137/2022 de 02/09/2022, em atendimento às disposições contidas na Lei Nº 10.520 de 17 de julho de 2002 e no Decreto Nº 10.024 de 20 de setembro de 2019, referente ao Processo Nº 16, para realizar os procedimentos relativos ao Pregão Nº 00001/2023. Modo de disputa: Aberto. Objeto: O objeto da presente licitação é a seleção da proposta mais vantajosa para a contratação de empresa especializada em SERVIÇOS GERENCIADOS DE SEGURANÇA, conforme condições e especificações estabelecidas no Anexo I – Termo de Referência deste Edital.. O Pregoeiro abriu a Sessão Pública em atendimento às disposições contidas no edital, divulgando as propostas recebidas. Abriu-se em seguida a fase de lances para classificação dos licitantes relativamente aos lances ofertados.

Item: 1

Descrição: Serviços de Consultoria em Tecnologia da Informação e Comunicação (TIC)

Descrição Complementar: Descrição detalhada no Anexo 1 - Termo de Referência do Edital 001/2023.

Tratamento Diferenciado: -

Quantidade: 1

Valor Máximo Aceitável: R\$ 872.250,0000

Aplicabilidade Decreto 7174: Não

Intervalo mínimo entre lances: R\$ 100,00

Unidade de fornecimento: UND SERVIÇO TÉCNICO

Situação: Cancelado no julgamento

Aplicabilidade Margem de Preferência: Não

Histórico

Item: 1 - Serviços de Consultoria em Tecnologia da Informação e Comunicação (TIC)

Propostas Participaram deste item as empresas abaixo relacionadas, com suas respectivas propostas.

(As propostas com * na frente foram desclassificadas)

CNPJ/CPF	Fornecedor	ME/EPP Equiparada	Declaração ME/EPP	Quantidade	Valor Unit.	Valor Global	Data/Hora Registro
17.067.013/0001-80	EGP SERVICOS LTDA	Sim	Sim	1	R\$ 900.000,0000	R\$ 900.000,0000	04/02/2023 08:45:30
Descrição Detalhada do Objeto Ofertado: SERVIÇOS GERENCIADOS DE SEGURANÇA Porte da empresa: ME/EPP							
01.707.536/0001-04	ISH TECNOLOGIA S/A	Não	Não	1	R\$ 2.901.450,0000	R\$ 2.901.450,0000	03/02/2023 15:58:11
Descrição Detalhada do Objeto Ofertado: Fornecimento de SERVIÇOS GERENCIADOS DE SEGURANÇA, conforme condições e especificações estabelecidas no Anexo I – Termo de Referência deste Edital. Porte da empresa: Demais (Diferente de ME/EPP)							

Lances (Obs: lances com * na frente indicam que foram excluídos)

Valor do Lance

CNPJ/CPF

Data/Hora Registro

R\$ 2.901.450,0000

01.707.536/0001-04

06/02/2023 09:40:00:400

R\$ 900.000,0000

17.067.013/0001-80

06/02/2023 09:40:00:400

R\$ 872.250,0000

17.067.013/0001-80

06/02/2023 09:56:23:157

R\$ 870.000,0000

17.067.013/0001-80

06/02/2023 10:11:44:140

Não existem lances de desempate ME/EPP para o item**Eventos do Item**

Evento	Data	Observações
Abertura	06/02/2023 09:55:00	Item aberto para lances.
Encerramento sem prorrogação	06/02/2023 10:05:01	Item aguardando decisão sobre reinício ou encerramento da etapa aberta.
Reinício etapa aberta	06/02/2023 10:08:36	Item com reinício da etapa aberta realizado. Justificativa: Tendo em vista que houve somente um lance na fase de disputa, objetivando uma melhor proposta para a administração..
Encerramento	06/02/2023 10:18:37	Item encerrado para lances.
Encerramento etapa aberta	06/02/2023 10:18:37	Item com etapa aberta encerrada.
Recusa de proposta	06/02/2023 10:51:22	Recusa da proposta. Fornecedor: EGP SERVICOS LTDA, CNPJ/CPF: 17.067.013/0001-80, pelo melhor lance de R\$ 870.000,0000. Motivo: Desclassificada de acordo com o que determina o item 5.1.2, tendo em vista que não foram inseridos no Comprasnet todos os documentos de habilitação exigidos, bem como não estão disponibilizados para consulta no SICAF, conforme requerido no item 5 do Edital.
Recusa de proposta	06/02/2023 11:13:24	Recusa da proposta. Fornecedor: ISH TECNOLOGIA S/A, CNPJ/CPF: 01.707.536/0001-04, pelo melhor lance de R\$ 2.901.450,0000. Motivo: Licitante desclassificada porque sua proposta estava acima do valor de referência e não houve interesse da mesma em negociar melhor proposta, conforme troca de mensagens via "chat" às 10:54:30 e 11:00:10 do dia 06/02/2023.
Cancelado no julgamento	06/02/2023 11:16:04	Item cancelado no julgamento. Motivo: Item 1 cancelado/fracassado por não ter havido proposta válida, conforme os motivos apresentados via "chat" e na opção "Julgamento de Propostas".

Não existem intenções de recurso para o item**Troca de Mensagens**

	Data	Mensagem
Sistema	06/02/2023 09:40:00	A sessão pública está aberta. Nesta compra haverá um período para a realização da análise de propostas e após este período os itens serão disponibilizados para o início dos lances. Até 20 itens poderão estar em disputa simultaneamente e o período de abertura para disputa será entre 08:00 e 18:00. Mantenham-se conectados.
Pregoeiro	06/02/2023 09:41:03	Prezadas licitantes, bom dia!
Pregoeiro	06/02/2023 09:41:20	Iniciarei dentro de instantes a fase de disputa (lances) do Pregão Eletrônico nº 001/2023, cujo objeto é a seleção da proposta mais vantajosa para a contratação de empresa especializada em SERVIÇOS GERENCIADOS DE SEGURANÇA.
Pregoeiro	06/02/2023 09:41:30	O CRCMG agradece a participação de todos!
Pregoeiro	06/02/2023 09:41:43	Antes de iniciar a fase de disputa (lances), enviarei algumas regras importantes para o bom atendimento dessa sessão pública. Solicito atenção as mensagens.
Pregoeiro	06/02/2023 09:41:54	O pregoeiro terá, inicialmente, 15 minutos para analisar as propostas de preços, podendo ser prorrogado, se necessário.
Pregoeiro	06/02/2023 09:42:10	As propostas serão julgadas de acordo com a sistemática do Comprasnet, em consonância com a legislação vigente.

Pregoeiro	06/02/2023 09:42:24	A comunicação entre o Pregoeiro e as licitantes será realizada, exclusivamente, por meio das ferramentas disponíveis no sistema Comprasnet, sendo vedado qualquer atendimento presencial ou por meio de ligações telefônicas.
Pregoeiro	06/02/2023 09:42:41	Caberá à licitante, acompanhar as operações no sistema eletrônico durante a sessão, obrigando-se a responder as solicitações do Pregoeiro via "chat", ficando responsável pelo ônus decorrente da perda de negócios diante de sua ausência de manifestação, pela inobservância de quaisquer mensagens emitidas ou de sua desconexão.
Pregoeiro	06/02/2023 09:42:55	A licitação será realizada em único item e o critério de julgamento adotado será o MENOR PREÇO DO ITEM.
Pregoeiro	06/02/2023 09:43:20	A proposta com a descrição do objeto ofertado e o preço, bem como os documentos de habilitação previstos no item 10 do Edital devem estar disponibilizados previamente no Comprasnet para serem consultados logo após o encerramento da fase de disputa, conforme disposto no item 5 do Edital e seus subitens. Também é permitido que os documentos de habilitação estejam disponíveis no SICAF para consulta.
Pregoeiro	06/02/2023 09:43:32	Caso os documentos não estejam disponíveis ou estiverem em desacordo ao exigido no Edital, implicará na desclassificação da licitante (item 5.1.2 do Edital).
Pregoeiro	06/02/2023 09:43:42	Cada lance deverá ser de no mínimo R\$ 100,00 (item 7.8 do Edital).
Pregoeiro	06/02/2023 09:43:53	Será adotado para o envio de lances o modo de disputa "aberto" (item 7.9 do Edital).
Pregoeiro	06/02/2023 09:43:59	A etapa de disputa terá duração de 10 minutos, após esse tempo, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos 2 minutos. Não havendo novos lances na forma estabelecida, a sessão pública encerrará automaticamente.
Pregoeiro	06/02/2023 09:44:19	Poderá ocorrer reinício da sessão pública de disputa, em prol da consecução do melhor preço, caso o pregoeiro e equipe de apoio julgarem necessário.
Pregoeiro	06/02/2023 09:44:26	Finalizada a fase de disputa e depois de verificado o atendimento ao item 7.27 (disponibilização prévia da proposta de preços e documentos de habilitação, conforme exigido no item 5), será encaminhada via chat contraproposta à licitante que apresentar melhor preço, objetivando uma proposta mais vantajosa (Negociação – item 7.28 do Edital).
Pregoeiro	06/02/2023 09:44:50	Ao ser solicitado o envio da Proposta de Preços ajustada ao último lance ofertado ou valor negociado, sugiro que seja utilizado o modelo proposto no Anexo II do Edital, objetivando evitar erros e agilizar o processo. Fiquem atentos às informações obrigatórias exigidas, como, identificação, preços ofertados, assinaturas, etc
Pregoeiro	06/02/2023 09:44:58	Para realizar a etapa de aceitabilidade da proposta vencedora, a proposta classificada será analisada pelo pregoeiro, equipe de apoio e pelo setor requisitante ou técnico (item 9 do Edital e seus subitens), o que poderá ocasionar em suspensão temporária da sessão para realizar o procedimento.
Pregoeiro	06/02/2023 09:45:16	Antes de efetivar a habilitação, serão realizadas consultas ao SICAF, TCU, CEIS e CNJ (item 10.1 do Edital) para apurar se existe alguma sanção impeditiva que descumpra a condição de participação, em caso positivo, a proposta será recusada (item 10.1.7 do Edital).
Pregoeiro	06/02/2023 09:45:32	Recomendo o cumprimento dos prazos editalícios para encaminhamento da proposta de preços e dos documentos de habilitação complementares (quando necessário e solicitado), bem como tomar ciência de como solicitar prorrogação de prazo.
Pregoeiro	06/02/2023 09:45:47	Neste momento irei conferir as propostas iniciais, as quais deverão estar em conformidade com o Edital e com as especificações constantes no Termo de Referência e em seguida será aberta a fase de disputa (lances).
Pregoeiro	06/02/2023 09:46:06	Vale destacar que propostas iniciais com valores inexequíveis e/ou com identificação da licitante serão excluídas (item 7.2 do Edital).
Pregoeiro	06/02/2023 09:46:18	Na fase de lances, valores considerados inexequíveis serão excluídos para não prejudicar o andamento do certame.
Pregoeiro	06/02/2023 09:50:00	As propostas já foram analisadas, daqui 5 minutos será iniciada a fase de disputa. Boa sorte a todos!
Sistema	06/02/2023 09:55:00	Etapa de análise de propostas encerrada. A abertura de itens para disputa será iniciada. Mantenham-se conectados.
Sistema	06/02/2023 09:55:00	O item 1 foi aberto. Solicitamos o envio de lances.
Pregoeiro	06/02/2023 09:55:17	Prezadas licitantes, item 1 aberto para lances. Boa sorte!
Pregoeiro	06/02/2023 09:56:11	Como já mencionado, a duração da etapa de disputa (lances) é de 10 minutos, findado este prazo, caso haja novo lance antes de encerrados 2 minutos, o sistema automaticamente prorroga a fase de disputa por mais 2 minutos até que não

		haja mais interessados em ofertarem novos valores, ou seja, se não houver lances a cada 2 minutos a fase de disputa é encerrada.
Pregoeiro	06/02/2023 10:00:01	Prezadas licitantes, aproveitem o restante do prazo inicial de disputa para ofertarem lances competitivos, depois terão somente 2 minutos aleatórios para decidirem antes do encerramento automático.
Pregoeiro	06/02/2023 10:03:01	Prezadas licitantes, o CRCMG é uma autarquia pública, busca sempre a economicidade, os valores apresentados para o item 1 estão modestos, peço que melhorem seus lances para que nosso objetivo de proposta mais vantajosa seja atingido.
Sistema	06/02/2023 10:05:01	O item 1 está aguardando decisão de reinício ou encerramento da etapa aberta pelo pregoeiro.
Pregoeiro	06/02/2023 10:08:03	Irei reiniciar a disputa, tendo em vista que houve somente um lance na fase de disputa, objetivando uma melhor proposta para a administração.
Sistema	06/02/2023 10:08:36	A etapa aberta do item 1 foi reiniciada. Justificativa: Tendo em vista que houve somente um lance na fase de disputa, objetivando uma melhor proposta para a administração.. Solicitamos o envio de lances.
Sistema	06/02/2023 10:18:37	O item 1 está encerrado.
Pregoeiro	06/02/2023 10:19:06	Prezadas licitantes! A fase de disputa foi finalizada. Darei continuidade ao certame analisando a proposta de preços e os documentos de habilitação disponibilizados, conforme exigido no item 5 do Edital e em seguida prosseguirei para a fase de Negociação (item 7.28 do Edital).
Sistema	06/02/2023 10:19:10	A etapa de julgamento de propostas foi iniciada. Acompanhe essa etapa na funcionalidade "Acompanhar Julgamento / Habilitação / Admissibilidade".
Pregoeiro	06/02/2023 10:21:35	Peço a gentileza que aguardem, irei analisar se a proposta de preços e os documentos de habilitação foram anexados previamente e/ou estão disponíveis para consultas no SICAF, conforme item 5 do Edital.
Pregoeiro	06/02/2023 10:49:11	Para EGP SERVICOS LTDA - Prezada licitante, não foram inseridos no Comprasnet todos os documentos de habilitação exigidos, bem como não estão disponibilizados para consulta no SICAF, conforme requerido no item 5 do Edital, portanto, será desclassificada, de acordo com o que determina o item 5.1.2.
Pregoeiro	06/02/2023 10:50:05	Prezadas licitantes, diante da situação mencionada, irei neste instante desclassificar a licitante e iniciar as análises da próxima melhor classificada.
Pregoeiro	06/02/2023 10:54:30	Para ISH TECNOLOGIA S/A - Prezada licitante, antes de analisar seus documentos disponibilizados no Comprasnet e no SICAF, como o valor da sua proposta está bem acima do de referência, gentileza informar se tem disponibilidade de negociar conosco, tendo em vista que não é permitida a contratação do serviço acima do valor de referência.
01.707.536/0001-04	06/02/2023 11:00:10	Sr. Pregoeiro, os valores praticados para este certame são valores inexequíveis, não há condições de qualquer empresa prestar os serviços requeridos no edital pelos valores de referência informados.
Pregoeiro	06/02/2023 11:03:40	Para ISH TECNOLOGIA S/A - Tudo bem! Irei reportar essa situação ao setor requisitante para nova análise.
Pregoeiro	06/02/2023 11:08:49	Prezada licitantes, diante de ter havido somente duas empresas participantes do certame, sendo que a melhor classificada, desclassificada por falta de envio de documentos e a seguinte não teve condições de prestar os serviços de acordo com o valor de referência, irei recusar a proposta da segunda e consequentemente esse pregão será considerado fracassado.
Pregoeiro	06/02/2023 11:13:58	Prezadas licitantes, irei realizar o cancelamento do item neste instante.
Sistema	06/02/2023 11:16:04	Srs. Fornecedores, está aberto o prazo para registro de intenção de recursos para os itens/grupos na situação de 'aceito e habilitado' ou 'cancelado no julgamento'.
Pregoeiro	06/02/2023 11:18:35	Foi informado o prazo final para registro de intenção de recursos: 06/02/2023 às 11:39:00.
Pregoeiro	06/02/2023 11:23:13	Foi informado nova data de fechamento de prazo para registro de intenção de recurso: 06/02/2023 às 11:54:00.
Pregoeiro	06/02/2023 11:24:30	Desculpem, informei o prazo equivocadamente para as intenções de recursos, mas já corriji e informei novo prazo. Agradecido pela compreensão.
Pregoeiro	06/02/2023 11:57:16	Prezadas licitantes, não houve intenção de recursos, sendo assim irei encerrar a sessão e encaminhar a decisão de cancelamento do item 1 para a autoridade competente. O CRCMG agradece a participação de todos! Tenham um ótimo dia!

Eventos da Licitação

Evento	Data/Hora	Observações
Alteração equipe	25/01/2023 15:33:16	
Alteração equipe	25/01/2023 15:33:21	
Alteração equipe	25/01/2023 15:40:38	Pregoeiro Anterior: 04289618600-SERGIO ROBSON MAFRA . Pregoeiro Atual: 07588499664-MARIA CHRISTINA DE OLIVEIRA . Justificativa: Expediente Administrativo.
Alteração equipe	02/02/2023 13:32:43	Pregoeiro Anterior: 07588499664-MARIA CHRISTINA DE OLIVEIRA . Pregoeiro Atual: 04289618600-SERGIO ROBSON MAFRA . Justificativa: Substituição de Pregoeiro devido o anterior está indisponível para a operacionalização no dia da abertura do certame.
Abertura da sessão pública	06/02/2023 09:40:00	Abertura da sessão pública
Encerramento da análise de propostas	06/02/2023 09:55:00	Etapa de análise de propostas encerrada.
Julgamento de propostas	06/02/2023 10:19:10	Início da etapa de julgamento de propostas
Abertura do prazo	06/02/2023 11:16:04	Abertura de prazo para intenção de recurso
Fechamento do prazo	06/02/2023 11:18:35	Fechamento de prazo para registro de intenção de recurso: 06/02/2023 às 11:39:00.
Fechamento do prazo	06/02/2023 11:23:13	Fechamento de prazo para registro de intenção de recurso reagendado para: 06/02/2023 às 11:54:00. Justificativa: Havia informado o prazo erroneamente, assim, foi necessário informar novo prazo para corrigir o equívoco.

Após encerramento da Sessão Pública, os licitantes melhores classificados foram declarados vencedores dos respectivos itens. Foi divulgado o resultado da Sessão Pública e foi concedido o prazo recursal conforme preconiza o artigo 45 , do Decreto Nº 10.024 de 20 de setembro de 2019. Nada mais havendo a declarar, foi encerrada a sessão às 11:58 horas do dia 06 de fevereiro de 2023, cuja ata foi lavrada e assinada pelo Pregoeiro e Equipe de Apoio.

SERGIO ROBSON MAFRA
Pregoeiro Oficial

ANDREZA MAIA BITARAES
Equipe de Apoio

OTACILIO VALADARES CORDEIRO
Equipe de Apoio

RICARDO ANDRADE TONACO
Equipe de Apoio



Voltar



Pregão/Concorrência Eletrônica



Conselho Regional de Contabilidade de Minas Gerais

Termo de Adjudicação do Pregão

Nº 00001/2023

Às 11:58 horas do dia 06 de fevereiro de 2023, após analisado o resultado do Pregão nº 00001/2023, referente ao Processo nº 16, o Pregoeiro, Sr(a) SERGIO ROBSON MAFRA, ADJUDICA aos licitantes vencedores os respectivos itens, conforme indicado no quadro Resultado da Adjudicação.

****OBS:** Itens com recursos serão adjudicados pela Autoridade competente e constarão no termo de julgamento.

Resultado da Adjudicação

Item: 1

Descrição: Serviços de Consultoria em Tecnologia da Informação e Comunicação (TIC)

Descrição Complementar: Descrição detalhada no Anexo 1 - Termo de Referência do Edital 001/2023.

Tratamento Diferenciado: -

Aplicabilidade Decreto 7174: Não

Aplicabilidade Margem de Preferência: Não

Quantidade: 1

Valor Máximo Aceitável: R\$ 872.250,0000

Situação: Cancelado no julgamento

Unidade de fornecimento: UND SERVIÇO TÉCNICO

Intervalo Mínimo entre Lances: R\$ 100,00

Eventos do Item

Evento	Data	Observações
Cancelado no julgamento	06/02/2023 11:16:04	Item cancelado no julgamento. Motivo: Item 1 cancelado/fracassado por não ter havido proposta válida, conforme os motivos apresentados via "chat" e na opção "Julgamento de Propostas".

Fim do documento

Pregão/Concorrência Eletrônica

Conselho Regional de Contabilidade de Minas Gerais

Termo de Homologação do Pregão Eletrônico

Pregão Nº 00001/2023 - (Decreto Nº 10.024/2019)

Às 14:56 horas do dia 10 de fevereiro de 2023, após constatada a regularidade dos atos procedimentais, a autoridade competente, Sr. SUELY MARIA MARQUES DE OLIVEIRA, HOMOLOGA a adjudicação referente ao Processo nº 16, Pregão nº 00001/2023.

Resultado da Homologação**Item: 1****Descrição:** Serviços de Consultoria em Tecnologia da Informação e Comunicação (TIC)**Descrição Complementar:** Descrição detalhada no Anexo 1 - Termo de Referência do Edital 001/2023.**Tratamento Diferenciado:** -**Aplicabilidade Decreto 7174:** Não**Aplicabilidade Margem de Preferência:** Não**Quantidade:** 1**Valor Máximo Aceitável:** R\$ 872.250,0000**Situação:** Cancelado no julgamento**Unidade de fornecimento:** UND SERVIÇO TÉCNICO**Intervalo Mínimo entre Lances:** R\$ 100,00**Eventos do Item**

Evento	Data	Nome	Observações
Cancelado no julgamento	06/02/2023 11:16:04	-	Item cancelado no julgamento. Motivo: Item 1 cancelado/fracassado por não ter havido proposta válida, conforme os motivos apresentados via "chat" e na opção "Julgamento de Propostas".
Homologado	10/02/2023 14:56:20	SUELY MARIA MARQUES DE OLIVEIRA	

Fim do documento

EXTRATO DE CONTRATO

Ata de Registro de Preços nº 07/2022, Espécie: Ata de Registro de Preços. Órgão Gerenciador: Conselho Federal dos Representantes Comerciais, CNPJ/MF: 34.046.367/0001-68, Empresa Registrada: Sodexo Pass do Brasil Serviços e Comércio S.A. CNPJ/MF: 69.034.668/0001-56, Objeto: Contratação de empresa para fornecimento de cartão alimentação e refeição com chip eletrônico. Amparo Legal: Lei nº 8.666/1993 e Lei nº 10.520/2002 Valor da ata anual: R\$1.294.869,12. Data da Assinatura: 10 de fevereiro de 2023. Vigência: 10 de fevereiro de 2023 a 10 de fevereiro de 2024. Signatários: Archimedes Cavalcanti Júnior, pelo ÓRGÃO GERENCIADOR (CONFERE), e Giovana Vieira Alves (SODEXO PASS DO BRASIL SERVIÇOS E COMÉRCIO S.A.) pela empresa CADASTRADA. Pregão eletrônico em SRP nº 11/2022, Espécie: Contrato de Prestação de Serviços nº 03/23, Contratante: Conselho Federal dos Representantes Comerciais, CNPJ/MF: 34.046.367/0001-68, Contratada: Sodexo Pass do Brasil Serviços e Comércio S.A. CNPJ/MF: 69.034.668/0001-56, Objeto: Contratação de empresa para fornecimento de cartão alimentação e refeição com chip eletrônico. Amparo Legal: Lei nº 8.666/1993 e Lei nº 10.520/2002. Valor do contrato anual: R\$763.224,00. Data da Assinatura: 10 de fevereiro de 2023 Vigência: 10 de fevereiro de 2023 a 10 de fevereiro de 2024. Signatários: Archimedes Cavalcanti Júnior, pelo CONTRATANTE (CONFERE), e Giovana Vieira Alves (SODEXO PASS DO BRASIL SERVIÇOS E COMÉRCIO S.A.) pela CONTRATADA.

CONSELHO DE ARQUITETURA E URBANISMO DE GOIÁS

EXTRATO DE INEXIGIBILIDADE DE LICITAÇÃO

Processo nº: 1675444/2023. Objeto: contratação de empresa especializada para produção de 500 (quinhentos) exemplares personalizados do "MINIGUIA DO ARQUITETO URBANISTA RECÉM-FORMADO", conforme especificações e quantidades estabelecidas no Projeto Básico.Total de Itens Licitados: 00001. Fundamento Legal: caput do Art. 25º da Lei nº 8.666 de 21/06/1993. Justificativa: orientação para os arquitetos e urbanistas recém formados. Declaração de Inexigibilidade em 26/01/2023. LORENA MARQUETE DA SILVA. Presidente da Comissão Permanente de Licitação. Ratificação em 10/02/2023. FERNANDO CAMARGO CHAPADEIRO. Presidente do Conselho de Arquitetura e Urbanismo de Goiás. Valor Global: R\$ 31.575,00 (trinta e um mil, quinhentos e setenta e cinco reais). CONTRATADA: 27.446.740 SERENA FERREIRA COSTA, CNPJ: 27.446.740/0001-02.

CONSELHO DE ARQUITETURA E URBANISMO DO PARANÁ

AVISO DE REGISTRO DE PREÇOS

PREGÃO ELETRÔNICO Nº PE - 12/2022 - SRP 1/2023

O Conselho de Arquitetura e Urbanismo do Paraná vem, por meio deste, comunicar a contratação por pregão Eletrônico para composição de ATA de Registro de Preço - SRP 01/2023 para realização de Eventos do CAU/PR, com validade de doze (12) meses a contar de 10/02/2023, da Empresa ANA PAULA VIEIRA FURRIGO BELMONTE LTDA CNPJ 15.784.588/0001-99, que apresentou a melhor proposta para os lotes/itens 1, 2, 3, 4, 5, 6, 7 e 8. O valor total REGISTRADO é de R\$ 786.905,00 (Setecentos e oitenta e seis mil e novecentos e cinco reais) por todos os lotes e itens da ATA de Registro de Preço.

Curitiba-PR, 6 de fevereiro de 2023.
MILTON CARLOS ZANELATTO GONÇALVES
Presidente do Conselho

CONSELHO DE ARQUITETURA E URBANISMO DO RIO DE JANEIRO

EXTRATO DE TERMO ADITIVO AO CONTRATO

TERMO ADITIVO Nº 1

Contratada: GOLDCOM TELECOMUNICAÇÕES LTDA; CNPJ/MF: 23.566.982/0001-89; Processo nº 1213377/2020; Objeto: prorrogar a vigência do contrato administrativo celebrado por mais 03 (três) meses; Valor: R\$ 29.360,36; Vigência: 14.02.2023 até 13.05.2023.

EXTRATO DE TERMO ADITIVO AO CONTRATO

Termo Aditivo Nº01

Contratada: OBDI LOCAÇÃO DE VEÍCULOS LTDA; CNPJ/MF: 09.546.840/0001-29; Processo nº 1477430/2020; Objeto: prorrogar a vigência do contrato administrativo celebrado por mais 12 (doze) meses; Valor: R\$ 295.174,26; Vigência: 14.02.2023 até 13.02.2024.

CONSELHO REGIONAL DE ADMINISTRAÇÃO DO PARÁ

EXTRATO DO 3º TERMO ADITIVO

CONTRATADA: IMPLANTA INFORMÁTICA LTDA - CNPJ/MF nº 37.994.043/0001-40. OBJETO DO ADITIVO: Prorrogação do prazo por mais 12 (doze) meses, contados a partir de 05/01/2023 até 05/01/2024. FUNDAMENTO: art. 57, § 1º, II da Lei Federal n.º 8.666/93 e suas alterações. VALOR GLOBAL: R\$ 146.932,80(cento e quarenta e seis mil novecentos e trinta e dois reais e oitenta centavos).DA RATIFICAÇÃO: As demais cláusulas do contrato permanecem inalteradas e são pelo presente Termo Aditivo ratificadas.

CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

AVISO DE INEXIGIBILIDADE LICITAÇÃO

PROC. ADM Nº 2022/000225

O Conselho Regional de Contabilidade do Espírito Santo torna público, a contratação por Inexigibilidade de Licitação, de acordo com o art. 74 da Lei 14.133/21: Objeto: contratação de Instrutor para ministrar palestra com tema "Gestão de negócios: Como criar uma contabilidade de referência no mercado", durante a XXIV Convenção dos Contabilistas do ES & V SESCES - Seminário das Empresas de Serviços, Metodologia: Presencial, nos dias 10 a 12 de maio de 2023, carga horária da palestra: 01h aproximadamente. CNPJ nº: 32.886.411/0001-12. Valor: R\$12.000,00 (doze mil reais).

Vitória - ES, 6 de fevereiro de 2023.
CARLA CRISTINA TASSO
Presidente do Conselho

CONSELHO REGIONAL DE CONTABILIDADE DE MINAS GERAIS

AVISO DE LICITAÇÃO FRACASSADA
PREGÃO ELETRÔNICO Nº 1/2023

O Conselho Regional de Contabilidade de Minas Gerais torna público para o conhecimento dos interessados que o Pregão Eletrônico n.º 001/2023, cujo objeto consiste na prestação de Serviços Gerenciados de Segurança, restou fracassado, tendo em vista a desclassificação de uma licitante, por não atendimento aos requisitos de habilitação, e a apresentação de proposta de preços acima do valor de referência por outra licitante.

Belo Horizonte, 13 de fevereiro de 2023.
SUELY MARIA MARQUES DE OLIVEIRA
Presidente do Conselho

CONSELHO REGIONAL DE CONTABILIDADE DO RIO GRANDE DO NORTE

EXTRATO DE CONTRATO Nº 1/2023

Espécie: Contrato Administrativo nº 001/2023, firmado em 02 de janeiro de 2023, constante no Processo de Compras nº 2022/000233. Contratante: Conselho Regional de Contabilidade do Rio Grande do Norte, CNPJ: 08.027.948/0001-42. Contratado: Leandro Cabral de Medeiros, CNPJ: 22.571.682/0001-25. Objeto: Contratação de empresa especializada para a prestação de serviços técnicos na área de Engenharia de Segurança e Medicina do Trabalho, de modo a elaborar, implementar, cumprir, coordenar e executar os Documentos, Programas, Laudos, Avaliações e Exames, em conformidade com as Normas Regulamentadoras do Ministério do Trabalho e Emprego (MTE) e outras legislações pertinentes, para o Conselho Regional de Contabilidade do Rio Grande do Norte (CRC/RN). Valor: R\$ 6.052,00 (seis mil e cinquenta e dois reais). Vigência: 12 (doze) meses, a contar de 02/01/2023. Dispositivo Legal: Lei Federal nº 8.666/93, suas alterações e demais legislações aplicáveis à espécie.

AVISO DE LICITAÇÃO Nº 1/2023

A presente licitação tem como objeto a escolha da proposta mais vantajosa para a Contratação de empresa para fornecimento, administração e gerenciamento de Vale Alimentação e/ou Vale Refeição aos funcionários do Conselho Regional de Contabilidade do Rio Grande do Norte - CRC/RN, por meio de Cartão Magnético com Chip de Segurança, inicialmente por 12 (doze) meses, conforme Termo de Referência, Anexo I, deste Edital e seus anexos. O Conselho Regional de Contabilidade do Rio Grande do Norte, através da sua Comissão Permanente de Licitação, torna público que realizará em 06 de março de 2023, às 09 horas, realizará licitação para o objeto acima especificado. O edital com as especificações e seus anexos encontra-se à disposição dos interessados no site www.crcrn.org.br, no Portal da Transparência, na aba de Licitações ou na Av. Nevaldo Rocha, 4545, Tirol, Natal/RN, na Comissão Permanente de Licitações no período de 13 de fevereiro a 01 de março de 2023, no horário de 08 às 11h e das 13 às 17h. Informações pelo telefone (84) 3211- 8512/8505 ou pelo e-mail: cpl@crcrn.org.br.

DIOGO MAED DANTAS MAIA
Pregoeiro

EDITAL DE CHAMAMENTO PÚBLICO Nº 2/2023

O Presidente do Conselho Regional de Contabilidade do Rio Grande do Norte - CRCRN entidade de fiscalização do exercício profissional, criado pelo Decreto-Lei nº 9.295/1946, inscrito no CNPJ sob o nº 08.027.948/0001-42, com sede na Av. Nevaldo Rocha, 4545, Tirol, Natal - RN, torna público, para conhecimento dos interessados, que será realizado Chamamento Público para seleção e credenciamento de pessoas jurídicas voltadas ao programa de educação profissional continuada conforme as condições estabelecidas neste Edital, aplicando-se, subsidiariamente, as normas da Lei Federal nº 8.666/1993.O Processo é organizado e conduzido pelo CRCRN, cujo Edital e seus anexos estão disponíveis no endereço www.crcrn.org.br, bem como todo e qualquer esclarecimento com relação ao presente Edital, deverá ser feito pelo e-mail: desenprof@crcrn.org.br.

ANAILSON MÁRCIO GOMES

CONSELHO REGIONAL DE CONTABILIDADE DE SÃO PAULO

EXTRATO DE TERMO ADITIVO

ESPÉCIE: Aditivo. OBJETO: Assistência Odontológica. CONTRATADA: INSTITUTO DE PREVIDÊNCIA E ASSISTÊNCIA ODONTOLÓGICA LTDA - INPAO. VIGÊNCIA: 02 (dois) meses a partir de 1º de março de 2023. DATA DE ASSINATURA: 23 de janeiro de 2023.

CONSELHO REGIONAL DE CORRETORES DE IMÓVEIS DA 19ª REGIÃO

EXTRATO DE CONTRATO ADMINISTRATIVO Nº 11/2023

Dispensa de inexigibilidade de licitação

Contratante: Conselho Regional de Corretores de Imóveis de Mato Grosso. CNPJ/MF 14.921.282/0001-74. Contratado: LN Comércio de Eletrônicos - Ltda., inscrita sob o CNPJ nº 01.030.685/0001-81. Objeto: Contratação de aquisição de refil de tintas para impressora. Prazo de vigência: 27.01.2023 a 27.01.2024. Data da assinatura: 27.01.2023.

CONSELHO REGIONAL DE CORRETORES DE IMÓVEIS DA 2ª REGIÃO

EXTRATO DE TERMO ADITIVO

Espécie: 3º Termo Aditivo ao Contrato de Prestação de Serviços do Processo Secom nº 041/2020 - Pregão Eletrônico nº. 018/2022. Contratante: Conselho Regional de Corretores de Imóveis da 2ª Região. Contratada: Lithium Construções Ltda. Objeto: Aquisição e instalação de portão automático na Delegacia Regional de São José dos Campos - Alteração do prazo. Data da Assinatura: 02/02/2023. Das Assinaturas: José Augusto Viana Neto, Francisco Pereira Afonso e Rick Henderson Vieira de Souza.

EXTRATO DE TERMO DE COOPERAÇÃO TÉCNICA

Partícipes: Conselho Regional de Corretores de Imóveis da 2ª. Região - CRECISP e Prefeitura Municipal de Peruíbe. Objeto: O presente Termo de Convênio e Cooperação tem por objetivo o interesse público, mediante a articulação, interação e a conjugação de esforços entre as partes signatárias, visando a uma melhor implementação de suas atribuições legais, e, em especial, proporcionar a Prefeitura Municipal de Peruíbe, assessoramento técnico-científico em atividades que necessitem de assunção de responsabilidade técnica de avaliação imobiliária, com vistas a instruir procedimentos administrativos em relação ao seu patrimônio imobiliário. Vigência: 24 (vinte e quatro) meses. Data da Assinatura: 23.12.2022.

CONSELHO REGIONAL DE CORRETORES DE IMÓVEIS DA 4ª REGIÃO

AVISO DE LICITAÇÃO
PREGÃO ELETRÔNICO Nº 3/2023

PROCESSO LICITATÓRIO Nº 9/2023

O Conselho Regional de Corretores de Imóveis do Estado de Minas Gerais torna público, para conhecimento dos interessados, que realizará certame destinado à contratação de empresa especializada para prestação de serviços de coffee break nos eventos "Entrega de Carteiras Profissionais", a serem realizados nos dias 09 e 16 de março de 2023, na cidade de Uberlândia/MG, na modalidade Pregão Eletrônico, tipo Menor Preço Do Item. A Sessão Pública acontecerá às 10h00min, horário de Brasília/DF, do dia 01/03/2023, quando serão abertas e analisadas as propostas comerciais, através do site www.gov.br/compras. A abertura da fase de lances tem início previsto para às 11h00min, do mesmo dia. O Edital e seus anexos encontram-se disponíveis nos sites www.gov.br/compras e www.crecimg.gov.br, podendo, ainda, serem solicitados através dos e-mails jonas@crecimg.gov.br, alessandra@crecimg.gov.br e liliane@crecimg.gov.br.

Belo Horizonte, 13 de fevereiro de 2023.
ALESSANDRA CARDOSO DE SOUZA LUCAS
Presidente da Comissão

