

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, 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	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://portaldatransparencia.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.

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. 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	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 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 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/cominação 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
<ul style="list-style-type: none"> Analista de Segurança I 	<ul style="list-style-type: none"> 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

	<ul style="list-style-type: none"> Certificação em pelo menos uma das soluções escolhidas para atender o tópico SOBRE AS FERRAMENTAS A SEREM UTILIZADAS 	<p>Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC);</p> <p>Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação.</p> <p>Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.</p>
<ul style="list-style-type: none"> Analista de Segurança II 	<ul style="list-style-type: none"> CompTIA Security+ e/ou CompTIA CySA+ e/ou Certified Ethical Hacker 	<p>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);</p> <p>Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de SIEM e ATD.</p> <p>Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.</p>

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
<ul style="list-style-type: none"> Linux LPIC 1, Linux LPIC 2 ou Linux LPIC 3 CompTIA Security+ ou Certified Ethical Hacker 	<p>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);</p> <p>Conhecimento avançado em segurança da informação com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação.</p> <p>Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.</p>

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

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
<ul style="list-style-type: none"> Analista de Segurança I 	<ul style="list-style-type: none"> 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

	<ul style="list-style-type: none"> ISFS (Information Security Foundation) 	<p>da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC);</p> <p>Conhecimento pleno em segurança da informação, realizando monitoramento de disponibilidade de ambiente de segurança da informação, similares ao ambiente supracitado.</p> <p>Experiência comprovada de no mínimo 12 (doze) meses em tecnologia da informação.</p>
--	--	---

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	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
<p>Ao menos uma das certificações de segurança da informação:</p> <ul style="list-style-type: none"> • Project Management Professional (PMP); • Prince2 Practitioner Certificate in Project Management; • Professional Scrum Master I; 	<p>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);</p> <p>Conhecimento avançado em gerencia de projetos, com experiência mínima de 12 (doze) meses.</p>

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:

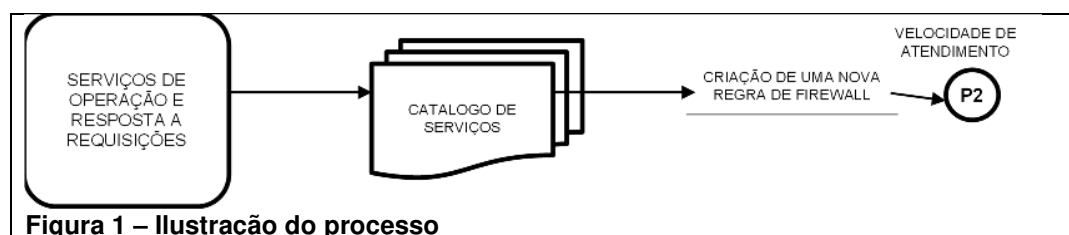


Figura 1 – Ilustração do processo

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
<p>Ao menos uma das certificações de segurança da informação:</p> <ul style="list-style-type: none"> • 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); 	<p>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);</p> <p>Conhecimento avançado em segurança da informação, com experiência mínima de 12 (doze) meses em coordenação e gestão de contratos de serviços continuados.</p>

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\$ (.....)

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

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:

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	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	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 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.

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	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

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
<p>Ao menos uma das certificações de segurança da informação:</p> <ul style="list-style-type: none"> • Project Management Professional (PMP); • Prince2 Practitioner Certificate in Project Management; • Professional Scrum Master I; 	<p>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);</p> <p>Conhecimento avançado em gerência de projetos, com experiência mínima de 12 (doze) anos.</p>

Tabela 1 - Qualificações Gerente de Projeto

2. Qualificações técnicas **PREPOSTO**:

Certificações	Descrição
<p>Ao menos uma das certificações de segurança da informação:</p> <ul style="list-style-type: none"> • 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); 	<p>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);</p> <p>Conhecimento avançado em segurança da informação, com experiência mínima de 5 (cinco) anos em coordenação e gestão de contratos de serviços continuados.</p>

Tabela 2 - Qualificações do Preposto

3. Qualificações técnicas do(s) **analista(s)** que participará do **GRUPO DE ATAQUE CIBERNÉTICO CONTROLADO (Red Team)**:

Certificações	Descrição
<ul style="list-style-type: none"> • CompTIA Security+ • CompTIA CySA+ 	<p>Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de</p>

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	<p>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);</p> <p>Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação.</p> <p>Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.</p>
---	--

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
<ul style="list-style-type: none"> • CompTIA Security+ e/ou • CompTIA CySA+ e/ou • Certified Ethical Hacker 	<p>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);</p> <p>Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de SIEM e ATD.</p> <p>Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.</p>

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
<ul style="list-style-type: none"> • CompTIA Security+ • CompTIA CySA+ • Certified Ethical Hacker • CompTIA Pentest+ ou • Computer Hacking Forensic Investigator 	<p>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);</p>

Nº PROCESSO ADMINISTRATIVO DE CONTRATAÇÃO	016/2023
MODALIDADE	Pregão Eletrônico
Nº DA MODALIDADE	001/2023

	<p>Especializações na área de segurança da informação.</p> <p>Conhecimento avançado em segurança da informação, com experiência em resposta a incidente de segurança da informação.</p> <p>Experiência comprovada de no mínimo 5 (cinco) anos em segurança da informação.</p>
--	---

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)