CRCMG
CONSELHO REGIONAL DE CONTABILIDADE DE MINAS GERAIS

CONTRATO DE PRESTAÇÃO DE SERVIÇOS

CONTRATO ADMINISTRATIVO QUE FAZEM ENTRE SI O CONSELHO REGIONAL DE CONTABILIDADE DE MINAS GERAIS (CRCMG) E A EMPRESA VOGEL SOLUÇÕES EM TELECOMUNICAÇÕES E INFORMÁTICA S/A.

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 sua presidente, Contadora Suely Maria Marques de Oliveira, doravante denominado CONTRATANTE, e a empresa **VOGEL SOLUÇÕES EM TELECOMUNICAÇÕES E INFORMÁTICA S/A**, inscrita no CNPJ/MF sob o nº 05.872.814/0001-30, sediada na Av. Professor Vicente Rao, nº 1262, Bairro Jardim Petrópolis, CEP: 04.636-001, São Paulo/SP, doravante designado CONTRATADO, neste ato representado por Jeankarlo Rodrigues da Cunha e Klever João dos Santos, conforme atos constitutivos da empresa, tendo em vista o que consta no Processo nº Administrativo de Contratação n.º 58/2025 e em observância às disposições da Lei nº 14.133, de 1º de abril de 2021, e demais legislação aplicável, resolvem celebrar o presente Termo de Contrato, decorrente Pregão Eletrônico nº 004//2025, mediante as cláusulas e condições a seguir enunciadas.

1. CLÁUSULA PRIMEIRA – OBJETO (art. 92, I e II)

1.1. Contratação de serviços de firewall de próxima geração (NGFW), Plataforma de Zero Trust (Confiança Zero) e Plataforma de gerenciamento, monitoramento e armazenamento de logs, incluindo demais serviços e treinamento Hands On, pelo período de 60 (sessenta) meses, conforme condições, quantidades e exigências estabelecidas neste instrumento e em seus anexos.

ITEM	ESPECIFICAÇÃO	UNIDADE DE MEDIDA	QTD
1	1.1 Firewall da Próxima Geração (NGFW);	Dispositivo (Mês)	1
	1.2 Plataforma de Zero Trust (Confiança Zero) para o mínimo de 100 usuários;	Usuários (Mês)	100
	1.3 Plataforma de gerenciamento, monitoramento e armazenamento de logs;	Dispositivo (Mês)	1
	1.4 Serviços profissionais de suporte técnico em toda solução;	Suporte técnico (Mês)	1
	1.5 Serviços profissionais de implementação da solução;	Implementação (Único)	1
	1.6 Operação assistida;	Operação assistida (Único)	5 dias
	1.7 Treinamento Hands On da operação do ambiente;	Usuários (Único)	2

1.2. São anexos a este instrumento e vinculam esta contratação, independentemente de transcrição:

1.2.1. O Termo de Referência;

1.2.2. O Edital da Licitação;

1.2.3. A Proposta do contratado;

1.2.4. Eventuais anexos dos documentos supracitados.

2. CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO.

2.1. O prazo de vigência da contratação é de 60 (sessenta) meses, contados da data de assinatura do contrato, prorrogável por até 10 (dez) anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

2.2. A prorrogação de que trata este item é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o contratado, atentando, ainda, para o cumprimento dos seguintes requisitos:

a) Estar formalmente demonstrado no processo que a forma de prestação dos serviços tem natureza continuada;

b) Seja juntado relatório que discorra sobre a execução do contrato, com informações de que os serviços tenham sido prestados regularmente;

c) Seja juntada justificativa e motivo, por escrito, de que a Administração mantém interesse na realização do serviço;

d) Haja manifestação expressa do contratado informando o interesse na prorrogação;

e) Seja comprovado que o contratado mantém as condições iniciais de habilitação.

2.3. O contratado não tem direito subjetivo à prorrogação contratual.

2.4. A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo.

2.5. Nas eventuais prorrogações contratuais, os custos não renováveis já pagos ou amortizados ao longo do primeiro período de vigência da contratação deverão ser reduzidos ou eliminados como condição para a renovação.

2.6. O contrato não poderá ser prorrogado quando o contratado tiver sido penalizado nas sanções de declaração de inidoneidade ou impedimento de licitar e contratar com poder público, observadas as abrangências de aplicação.

3. CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS (art. 92, IV, VII e XVIII)

3.1. O regime de execução contratual, o modelo de gestão, assim como os prazos e condições de conclusão, entrega, observação e recebimento definitivo constam no Termo de Referência, anexo a este Contrato.

4. CLÁUSULA QUARTA - SUBCONTRATAÇÃO

4.1. Não será admitida a subcontratação do objeto contratual.

5. CLÁUSULA QUINTA – PREÇO

5.1. Pela execução dos serviços, objeto deste contrato, o CRCMG pagará à contratada os valores discriminados nas tabelas abaixo:

ESPECIFICAÇÃO	UNIDADE DE MEDIDA	QTD	Preço	
1.1 Firewall da Próxima Geração (NGFW);	Dispositivo (Mês)	1	Mensal	R$ 2.690,00
1.2 Plataforma de Zero Trust (Confiança Zero) para o mínimo de 100 usuários;	Usuários (Mês)	100		R$ 2.000,00
1.3 Plataforma de gerenciamento, monitoramento e armazenamento de logs;	Dispositivo (Mês)	1		R$ 1.500,00
1.4 Serviços profissionais de suporte técnico em toda solução;	Suporte técnico (Mês)	1		R$ 1.500,00
Valor total dos serviços prestados mensalmente				**R$ 7.690,00**

ESPECIFICAÇÃO	UNIDADE DE MEDIDA	QTD	Preço	
1.5 Serviços profissionais de implementação da solução;	Implementação (Único)	5 dias	Parcela única	**R$ 0,00**
1.6 Operação assistida;	Operação assistida (Único)	1		**R$ 0,00**
1.7 Treinamento Hands On da operação do ambiente;	Usuários (Único)	2		**R$ 0,00**
Valor total dos serviços prestados em parcela única				**R$ 0,00**

Valor total dos serviços pelo período de 60 meses (somatório dos serviços mensais com serviços prestados em parcela única)	
Valor total dos serviços prestados mensalmente	**R$ 461.400,00**
Valor total dos serviços prestados em parcela única	**R$ 0,00**
VALOR TOTAL DOS SERVIÇOS PELO PERÍODO DE 60 MESES	**R$ 461.400,00**

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

6. CLÁUSULA SEXTA - CONDIÇÕES DE PAGAMENTO (art. 92, V e VI)

6.1. O prazo para pagamento ao Contratado e demais condições a ele referentes encontram-se definidos no Termo de Referência, anexo a este Contrato.

7. CLÁUSULA SÉTIMA - REAJUSTE (art. 92, V)

7.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, em 28/04/2025.

7.2. Após o interregno de um ano, desde que a pedido do contratado, os preços iniciais poderão ser reajustados, mediante a aplicação, pelo contratante, do IPCA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

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

7.4. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

7.5. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

7.6. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

7.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

7.8. O reajuste será realizado por apostilamento.

8. CLÁUSULA OITAVA - OBRIGAÇÕES DO CONTRATANTE (art. 92, X, XI e XIV)

8.1. São obrigações do Contratante:

8.1.1. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o contrato e seus anexos;

8.1.2. Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

8.1.3. Notificar o Contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;

8.1.4. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado;

8.1.5. Comunicar a empresa para emissão de Nota Fiscal em relação à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133, de 2021;

8.1.6. Efetuar o pagamento ao Contratado do valor correspondente ao fornecimento do objeto, no [redacted], forma e condições estabelecidos no Termo de Referência;

8.1.7. Aplicar ao Contratado sanções motivadas pela inexecução total ou parcial do Contrato;

8.1.8. Cientificar a Assessoria Jurídica para adoção das medidas cabíveis quando do descumprimento de obrigações pelo Contratado;

8.1.9. Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.

8.1.9.1. A Administração terá o prazo de 30 (trinta) dias, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.

8.1.9.2. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo contratado no prazo máximo de 30 (trinta) dias.

8.1.10. Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

8.1.11. Comunicar o Contratado na hipótese de posterior alteração do projeto pelo Contratante, no caso do art. 93, §2º, da Lei nº 14.133, de 2021.

8.1.12. A Administração não responderá por quaisquer compromissos assumidos pelo Contratado com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do Contratado, de seus empregados, prepostos ou subordinados.

9. CLÁUSULA NONA - OBRIGAÇÕES DO CONTRATADO (art. 92, XIV, XVI e XVII)

9.1. O Contratado deve cumprir todas as obrigações constantes deste Contrato, em seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:

9.1.1. Indicar preposto aceito pela Administração para representá-lo na execução do contrato.

9.1.2. A indicação ou a manutenção do preposto da empresa poderá ser recusada pelo órgão ou entidade, desde que devidamente justificada, devendo a empresa designar outro para o exercício da atividade.

9.1.3. Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior (art. 137, II);

9.1.4. Alocar os empregados necessários ao perfeito cumprimento deste contrato, com habilitação e conhecimento adequados, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência;

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

9.1.6. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo Contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida, o valor correspondente aos danos sofridos;

9.1.7. Não contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do contratante ou do Fiscal ou Gestor do contrato, nos termos do artigo 48, parágrafo único, da Lei nº 14.133, de 2021;

9.1.8. Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, o contratado deverá entregar ao setor responsável pela fiscalização do contrato, até o dia trinta do mês seguinte ao da prestação dos serviços, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda Estadual e/ou Municipal ou Distrital do domicílio ou sede do contratado; 4) Certidão Negativa de Débitos Trabalhistas – CNDT;

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

9.1.10. Prestar todo esclarecimento ou informação solicitada pelo Contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo aos documentos relativos à execução do empreendimento;

9.1.11. Paralisar, por determinação do Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros;

9.1.12. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos;

9.1.13. Submeter previamente, por escrito, ao Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congênere;

9.1.14. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;

9.1.15. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação e qualificação, na contratação direta;

9.1.16. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação (art. 116);

9.1.17. Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas (art. 116, parágrafo único);

9.1.18. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

[redacted]. 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 contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, II, d, da Lei nº 14.133, de 2021.

9.1.20. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do Contratante.

9.1.21. Realizar a transição contratual com transferência de conhecimento, visando à preservação e manutenção dos serviços.

10. CLÁUSULA DÉCIMA - OBRIGAÇÕES PERTINENTES À LGPD

10.1. 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.

10.2. 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 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.

10.3. 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.

10.4. 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.

10.5. 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.

10.6. Ressalvado o disposto no item 10.7, 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.

10.7. 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).

10.7.1. 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).

10.7.2. 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.

10.8. 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.

10.9. 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 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;

10.10. 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.

10.11. 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.

10.12. 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.

10.13. Eventualmente, as partes podem ajustar que o CONTRATANTE será responsável por obter o consentimento dos titulares, observadas as demais condicionantes no item 10.11 acima.

10.14. 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 con[redacted]s.

10.15. 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.

11. CLÁUSULA DÉCIMA PRIMEIRA – GARANTIA DE EXECUÇÃO (art. 92, XII e XIII)

11.1. O contratado apresentará, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do contratante, contado da assinatura do contrato, comprovante de prestação de garantia, podendo optar por caução em dinheiro ou títulos da dívida pública ou, ainda, pela fiança bancária, em valor correspondente a correspondente a 5% (cinco por cento) do valor inicial total do contrato.

11.2. Caso utilizada a modalidade de seguro-garantia, a apólice deverá ter validade durante a vigência do contrato e por mais 90 (noventa) dias após término deste prazo de vigência, permanecendo em vigor mesmo que o contratado não pague o prêmio nas datas convencionadas.

11.3. A apólice do seguro garantia deverá acompanhar as modificações referentes à vigência do contrato principal mediante a emissão do respectivo endosso pela seguradora.

11.4. Será permitida a substituição da apólice de seguro-garantia na data de renovação ou de aniversário, desde que mantidas as condições e coberturas da apólice vigente e nenhum período fique descoberto, ressalvado o disposto no item 11.5 deste contrato.

11.5. Na hipótese de suspensão do contrato por ordem ou inadimplemento da Administração, o contratado ficará desobrigado de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pela Administração.

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

11.6.1. prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;
11.6.2. multas moratórias e punitivas aplicadas pela Administração à contratada; e
11.6.3. obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pelo contratado, quando couber.

11.7. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item 11.6 observada a legislação que rege a matéria.

11.8. A garantia em dinheiro deverá ser efetuada em favor do contratante, em conta específica na Caixa Econômica Federal, com correção monetária.

11.9. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Economia.

11.10. No caso de garantia na modalidade de fiança bancária, deverá ser emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil, e deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

11.11. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.

11.12. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, o Contratado obriga-se a fazer a respectiva reposição no prazo máximo de 10 (dez) dias úteis, contados da data em que for notificada.

11.13. O Contratante executará a garantia na forma prevista na legislação que rege a matéria.

11.13.1. O emitente da garantia ofertada pelo contratado deverá ser notificado pelo contratante quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais (art. 137, § 4º, da Lei n.º 14.133, de 2021).

11.13.2. Caso se trate da modalidade seguro-garantia, ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos do art. 20 da Circular Susep n° 662, de 11 de abril de 2022.

11.14. Extinguir-se-á a garantia com a restituição da apólice, carta fiança ou autorização para a liberação de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do contratante, mediante termo circunstanciado, de que o contratado cumpriu todas as cláusulas do contrato;

11.15. A garantia somente será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da Administração e, quando em dinheiro, será atualizada monetariamente.

11.16. O garantidor não é parte para figurar em processo administrativo instaurado pelo contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada.

11.17. O contratado autoriza o contratante a reter, a qualquer tempo, a garantia, na forma prevista neste Contrato.

11.18. A garantia de execução é independente de eventual garantia do produto ou serviço prevista especificamente no Termo de Referência.

12. CLÁUSULA DÉCIMA SEGUNDA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS (art. 92, XIV)

12.1. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o Contratado que:

a) der causa à inexecução parcial do contrato;

b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

c) der causa à inexecução total do contrato;

d) deixar de entregar a documentação exigida para o certame;

e) não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

f) não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

g) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

h) apresentar declaração ou documentação falsa exigida para a contratação ou prestar declaração falsa durante a execução do contrato;

i) fraudar a contratação ou praticar ato fraudulento na execução do contrato;

j) [redacted]portar-se de modo inidôneo ou cometer fraude de qualquer natureza;

k) praticar atos ilícitos com vistas a frustrar os objetivos da contratação;

l) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

12.2. Serão aplicadas ao responsável pelas infrações administrativas acima descritas as seguintes sanções:

i) **Advertência**, quando o Contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei);

ii) **Impedimento de licitar e contratar**, quando praticadas as condutas descritas nas alíneas b, c, d, e, f e g do subitem acima deste Contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §4º, da Lei);

iii) **Declaração de inidoneidade para licitar e contratar**, quando praticadas as condutas descritas nas alíneas h, i, j, k e l do subitem acima deste Contrato, bem como nas alíneas b, c, d, e, f e g, que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei)

iv) **Multa:**

(1) moratória de 0,5 % (cinco décimos por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 15 (quinze) dias;

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

12.3. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Contratante (art. 156, §9º)

12.4. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º).

12.4.1. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157)

12.4.2. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será cobrada judicialmente (art. 156, §8º).

12.4.3. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 10 (dez) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

12.5. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no **caput** e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

12.6. Na aplicação das sanções serão considerados (art. 156, §1º):

a) a natureza e a gravidade da infração cometida;
b) as peculiaridades do caso concreto;
c) as circunstâncias agravantes ou atenuantes;
d) os danos que dela provierem para o Contratante;
e) a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

12.7. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de

2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159).

12.8. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160, da Lei nº 14.133, de 2021).

12.9. O Contratante deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal. (Art. 161)

12.10. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21.

12.11. Os débitos do contratado para com a Administração contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o contratado possua com o mesmo órgão ora contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

13. CLÁUSULA DÉCIMA TERCEIRA – DA EXTINÇÃO CONTRATUAL (art. 92, XIX)

13.1. O contrato se extingue quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes.

13.1.1. O contrato poderá ser extinto antes do prazo nele fixado, sem ônus para o Contratante, quando esta não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

13.1.2. A extinção nesta hipótese ocorrerá na próxima data de aniversário do contrato, desde que haja a notificação do contratado pelo contratante nesse sentido com pelo menos 2 (dois) meses de antecedência desse dia.

13.1.3. Caso a notificação da não continuidade do contrato de que trata este subitem ocorra com menos de 2 (dois) meses da data de aniversário, a extinção contratual ocorrerá após 2 (dois) meses da data da comunicação.

13.2. O contrato pode ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da NLLC, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

[redacted]. Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei.

13.2.2. A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a extinção se não restringir sua capacidade de concluir o contrato.

13.2.2.1. Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

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

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

13.3.2. Relação dos pagamentos já efetuados e ainda devidos;

13.3.3. Indenizações e multas.

13.4. O contrato poderá ser extinto caso se constate que o contratado mantém vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que tenha desempenhado função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau (art. 14, inciso IV, da Lei n.º 14.133, de 2021).

14. CLÁUSULA DÉCIMA QUARTA – DOTAÇÃO ORÇAMENTÁRIA (art. 92, VIII)

14.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no orçamento do CRCMG deste exercício, na dotação abaixo discriminada:

I. Projeto: 5002 – Tecnologia da Informação

II. Conta contábil: 6.3.1.3.02.01.005 – Serviços de Tecnologia da Informação

III. Centro de custo: 327 – Gerência de Tecnologia da Informação

15. CLÁUSULA DÉCIMA QUINTA – DOS CASOS OMISSOS (art. 92, III)

15.1. Os casos omissos serão decididos pelo contratante, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

16. CLÁUSULA DÉCIMA SEXTA – ALTERAÇÕES

16.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021.

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

16.3. As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia aprovação da consultoria jurídica do contratante, salvo nos casos de justificada necessidade de antecipação de seus efeitos, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 1 (um) mês (art. 132 da Lei nº 14.133, de 2021).

16.4. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de 2021.

17. CLÁUSULA DÉCIMA SÉTIMA – PUBLICAÇÃO

17.1. Incumbirá à CONTRATANTE providenciar a publicação deste instrumento nos termos e condições previstas na Lei nº 14.133/21.

18. CLÁUSULA DÉCIMA OITAVA - DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO CRCMG

18.1. O Contratado 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.

19. CLÁUSULA DÉCIMA NONA – DA ASSINATURA ELETRÔNICA/DIGITAL

19.1. 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.

19.2. 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.

20. CLÁUSULA VIGÉSIMA – FORO (art. 92, §1º)

20.1. É eleito o Foro da Justiça Federal - Subseção de Belo Horizonte para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não possam ser compostos pela conciliação, conforme art. 92, §1º da Lei nº 14.133/21.

Belo Horizonte, 27 de maio de 2025.

Assinado digitalmente por:
SUELY MARIA MARQUES DE OLIVEIRA
CPF: [redacted]
Certificado emitido por AC SOLUTI Multipla v5
Data: 28/05/2025 15:43:14 -03:00

CONSELHO REGIONAL DE CONTABILIDADE DE MINAS GERAIS
Suely Maria Marques de Oliveira
Presidente do CRCMG

Assinado digitalmente por:
JEANKARLO RODRIGUES DA CUNHA
CPF [redacted]
Certificado emitido por AC SAFEWEB RFB v5
Data: 28/05/2025 15:09:09 -03:00

VOGEL SOLUÇÕES EM TELECOMUNICAÇÕES E INFORMÁTICA S/A
P/p. Jeankarlo Rodrigues da Cunha
Representante legal

Assinado digitalmente por:
KLEVER JOAO DOS SANTOS
CPF [redacted]
Certificado emitido por AC ONLINE RFB v5
Data: 28/05/2025 08:38:56 -03:00

VOGEL SOLUÇÕES EM TELECOMUNICAÇÕES E INFORMÁTICA S/A
P/p. Klever João dos Santos
Representante legal

Testemunhas:

1ª
Assinado digitalmente por:
CLAUDIO MARCIO ARAUJO DA SILVA
CPF: [redacted]
Certificado emitido por AC SyngularID Multipla
Data: 28/05/2025 15:12:31 -03:00

2ª
Assinado digitalmente por:
WATSON BONIFACIO DA SILVA
CPF: [redacted]
Certificado emitido por AC SyngularID Multipla
Data: 28/05/2025 15:10:38 -03:00

Assinado digitalmente por:
WILLIAN FERNANDO DE FREITAS
CPF: [redacted]
Certificado emitido por AC SAFEWEB RFB v5
Data: 28/05/2025 15:34:56 -03:00
Visto do Jurídico do CRCMG

ANEXO I - TERMO DE REFERÊNCIA

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Contratação de serviços de firewall de próxima geração (NGFW), Plataforma de Zero Trust (Confiança Zero) e Plataforma de gerenciamento, monitoramento e armazenamento de logs, incluindo demais serviços e treinamento Hands On, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

ITEM	ESPECIFICAÇÃO	CATSER	UNIDADE DE MEDIDA	QTD	VALOR MENSAL + PERCELA ÚNICA	VALOR TOTAL ESTIMADO – 60 MESES
1	1.1 Firewall da Próxima Geração (NGFW); Modelo de referência: FG-90G da Fortinet (equivalente ou superior)	609340	Dispositivo (Mês)	1	R$ 8.725,00	R$ 523.500,00
	1.2 Plataforma de Zero Trust (Confiança Zero) para o mínimo de 100 usuários;		Usuários (Mês)	100		
	1.3 Plataforma de gerenciamento, monitoramento e armazenamento de logs;		Dispositivo (Mês)	1		
	1.4 Serviços profissionais de suporte técnico em toda solução;		Suporte técnico (Mês)	1		
	1.5 Serviços profissionais de implementação da solução;		Implementação (Único)	1		
	1.6 Operação assistida;		Operação assistida (Único)	5 dias		
	1.7 Treinamento Hands On da operação do ambiente;		Usuários (Único)	2		

1.2. Os serviços objeto desta contratação são caracterizados como comuns, considerando que as especificações constam definidas objetivamente neste instrumento.

1.3. O prazo de vigência da contratação é de 60 meses contados da assinatura do contrato, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

1.4. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. Constitui a necessidade da contratação o fornecimento de solução de segurança robusta, que inclui um firewall de próxima geração (NGFW), uma plataforma de Zero Trust e uma plataforma para gerenciamento, monitoramento e armazenamento de logs. O NGFW tem por objetivo a proteção contra ameaças cibernéticas e acessos não autorizados, enquanto a plataforma de Zero Trust garantirá que apenas usuários e dispositivos confiáveis tenham acesso à rede. A plataforma de logs permitirá o registro e a análise de eventos para facilitar o monitoramento e a investigação de incidentes de segurança. Além disso, deverão ser oferecidos serviços profissionais para implementação, monitoramento contínuo, gerenciamento e treinamento prático para a equipe técnica.

2.2. Com o contrato atual expirando em fevereiro de 2025, essa nova contratação visa assegurar a proteção contínua das informações e infraestrutura, otimizar recursos e garantir suporte especializado contra ameaças cibernéticas, mantendo a rede segura e em conformidade com as melhores práticas de segurança da informação.

2.3. A adoção do Firewall como Serviço permitirá a otimização dos recursos, a redução de custos com hardware e manutenção, e garantirá que a infraestrutura de TI esteja preparada para enfrentar as ameaças atuais e futuras de maneira eficiente, oferecendo maior flexibilidade e escalabilidade à medida que as necessidades de segurança evoluem.

2.4. A contratação visa permitir ao CRCMG o desempenho de suas atribuições institucionais, conforme dispõe Decreto-Lei n.º 9.295/1946.

2.5. O objeto da contratação está previsto no Plano de Contratações Anual 2025, conforme consta das informações básicas deste termo de referência.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

3.1. A solução proposta abrange a contratação de serviços especializados para a implementação e gestão de um firewall de próxima geração (NGFW) e de uma plataforma de Zero Trust (Confiança Zero), juntamente com a plataforma de gerenciamento, monitoramento e armazenamento de logs.

3.2. O objetivo é assegurar a proteção, o monitoramento e o controle da infraestrutura de TI do CRCMG.

3.3. A solução de firewall de próxima geração (NGFW) será responsável pela proteção da rede, servidores e dados contra acessos não autorizados e ameaças cibernéticas, além de permitir a aplicação de políticas de segurança avançadas. Essa ferramenta oferece funcionalidades como detecção e prevenção de intrusões (IDS/IPS), filtragem de conteúdo, controle de aplicações e gerenciamento centralizado de ameaças. Com isso, o CRCMG poderá garantir que todo o tráfego de rede seja devidamente monitorado e que as políticas de segurança sejam aplicadas de forma consistente.

3.4. A plataforma de Zero Trust (Confiança Zero) será responsável por garantir a segurança da rede, servidores e dados ao adotar uma abordagem baseada na premissa de que nenhuma entidade, seja interna ou externa, deve ser automaticamente confiável. Essa solução implementa mecanismos de verificação contínua de identidade e autorização, microsegmentação de rede, controle rigoroso de acesso e monitoramento em tempo real de atividades suspeitas. Com essa ferramenta, o CRCMG poderá assegurar que todos os acessos e movimentos laterais dentro da rede sejam rigorosamente controlados e autenticados, aplicando políticas de segurança de maneira consistente e reduzindo significativamente os riscos de ameaças internas e externas.

3.5. Complementarmente, a plataforma de gerenciamento, monitoramento e armazenamento de logs permitirá a coleta, o armazenamento e a análise de eventos relacionados à segurança da rede. Esses logs também serão utilizados pela empresa contratada de monitoramento e segurança de rede auxiliando na detecção de atividades suspeitas e facilitando a investigação de eventos de segurança. A solução garante uma auditoria contínua da rede, proporcionando maior visibilidade sobre o ambiente de TI e permitindo que ações corretivas sejam tomadas de forma ágil.

3.6. Toda a infraestrutura será gerenciada pela empresa contratada, que será responsável pela administração completa da solução, garantindo a atualização contínua das políticas de segurança e

monitoramento. Além disso, será oferecido treinamento específico aos usuários indicados pelo CRCMG para a operação da plataforma de gerenciamento, monitoramento e armazenamento de logs, visando capacitar a equipe interna na geração de relatórios e análise dos dados de segurança.

3.7. A solução como um todo busca assegurar a proteção contra ameaças cibernéticas, garantir a integridade e confidencialidade dos dados, e proporcionar a visibilidade e controle necessários para a gestão eficiente da segurança da informação no CRCMG. A empresa contratada será responsável tanto pela instalação e configuração dos equipamentos quanto pelo suporte técnico contínuo, assegurando que a solução esteja sempre em pleno funcionamento e ajustada às necessidades da instituição.

4. REQUISITOS DA CONTRATAÇÃO

Sustentabilidade

4.1. Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto e no Guia Nacional de Contratações Sustentáveis da Advocacia-Geral da União, a contratada deve adotar as seguintes práticas de sustentabilidade na execução dos serviços, no que couber:

a) Observar a legislação obrigatória que trata das práticas de sustentabilidade ambiental nas contratações com Administração Pública, especialmente, em relação à Lei nº 12.305, de 2 de agosto de 2010; ao Decreto nº 10.936, de 12 de janeiro de 2022 e à IN/SLTI/MP nº 1, de 19 de janeiro de 2010;
b) Respeitar as Normas Brasileiras – NBR publicadas pela Associação Brasileira de Normas Técnicas sobre resíduos sólidos;
c) Que os bens sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR – 15448-1 e 15448-2;
d) Que sejam observados os requisitos ambientais para a obtenção de certificação do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial – INMETRO como produtos sustentáveis ou de menor impacto ambiental em relação aos seus similares;
e) Que os bens devam ser, preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento; e
f) Que os bens não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenil-polibromados (PBBs), éteres difenil-polibromados (PBDEs).

Indicação de marcas ou modelos

4.2. Na presente contratação não será admitida a indicação de marca.

Subcontratação

4.3. Não é admitida a subcontratação do objeto contratual.

Garantia da contratação

4.4. Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, podendo o Contratado optar pela caução em dinheiro ou em títulos da dívida pública, seguro-garantia,

fiança bancária ou título de capitalização, em valor correspondente a 5% (cinco por cento) do valor total da contratação.

4.5. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

Vistoria

4.6. A contratada deverá apresentar Atestado de Vistoria ou Declaração de Ciência das Condições do local, conforme o seguinte:

4.6.1. A avaliação prévia do local de execução dos serviços é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, sendo assegurado ao interessado o direito de realização de vistoria prévia, acompanhado por servidor designado para esse fim, de segunda à sexta-feira, das 9 horas às 17 horas.

4.6.2. Serão disponibilizados data e horário diferentes aos interessados em realizar a vistoria prévia.

4.6.3. A vistoria poderá ser agendada pelo e-mail licitacao@crcmg.org.br.

4.6.4. Para a vistoria, o representante legal da empresa ou responsável técnico deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria.

4.6.5. Caso o licitante opte por não realizar a vistoria, deverá prestar declaração formal assinada pelo responsável técnico do licitante acerca do conhecimento pleno das condições e peculiaridades da contratação.

4.6.6. A não realização da vistoria não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo o contratado assumir os ônus dos serviços decorrentes.

4.6.7. O Atestado de Vistoria e a Declaração de Ciência das Condições do Local de Execução constam dos anexos do edital.

5. MODELO DE EXECUÇÃO DO OBJETO

Condições de execução

5.1. A execução do objeto seguirá a seguinte dinâmica:

5.2. Início da execução do objeto: a prestação do serviço, com a completa entrada em operação da solução, deverá ter início em até 90 dias, contado da assinatura do contrato.

5.3. Cronograma de realização dos serviços:

a) Após a assinatura do contrato, ambas as partes deverão agendada uma reunião de alinhamento para definição e elaboração de cronograma de implantação.
b) Nessa mesma reunião, a Contratada deverá apresentar o cronograma, que estará sujeito à aprovação da Contratante.

5.4. Serão de responsabilidade da CONTRATADA as atividades de instalação, integração, configuração e testes de todos os produtos componentes de cada Solução de Segurança;

5.5. A CONTRATADA deverá levantar informações acerca dos locais de instalação dos produtos, e, se necessário, efetuar visita técnica para verificar eventuais requisitos físicos a serem providos para a correta instalação e prestação dos serviços;

5.6. A conclusão da fase de implantação dos serviços é de até 90 (noventa) dias corridos, contados a partir da data de assinatura do contrato.

5.7. Estimar o consumo de Unidades de Rack (U) e de energia de cada ativo a ser instalado nas dependências da CONTRATANTE;

5.8. Os Softwares e demais componentes necessários à correta prestação dos serviços deverão:

5.9. 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;

5.10. Conter a última versão de Software e Firmware homologado pelo fabricante;

5.11. 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);

5.12. Quando houver atualizações 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;

5.13. A operação assistida deverá obedecer aos requisitos a seguir:

5.14. Iniciará quando forem finalizadas as disponibilizações do serviço;

5.15. 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;

5.16. 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;

5.17. 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.

5.18. 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.

Local e horário da prestação dos serviços

5.19. Os serviços serão prestados no seguinte endereço Rua Cláudio Manoel, 639 – Bairro Savassi, em Belo Horizonte/MG.

5.20. Os serviços serão prestados de forma integral, 24 horas por dia, 7 dias por semana.

Rotinas a serem cumpridas

5.21. A execução contratual observará as rotinas abaixo:

5.21.1. Disponibilização, instalação e configuração de Firewall de Próxima Geração (NGFW);

5.21.2. Fornecer plataforma de Zero Trust (Confiança Zero) necessária em nuvem própria ou nuvem pública.

5.21.3. Fornecer plataforma para o gerenciamento, monitoramento e armazenamento de logs.

5.21.4. Fornecer plataforma de multifator de autenticação.

5.21.5. Fornecer treinamento prático (hands-on) para capacitar a equipe do CRCMG no uso e operação das plataformas e do firewall instalado.

5.21.6. Fornecer RMA do equipamento Firewall da Próxima Geração (NGFW).

5.21.7. Prover suporte de operação assistida para auxiliar o CRCMG nos primeiros meses de uso, garantindo o correto funcionamento e entendimento das soluções.

5.21.8. Fornecer suporte técnico para resolver quaisquer problemas ou dúvidas, garantindo o funcionamento contínuo e seguro das soluções de segurança, gerenciamento e monitoramento implantadas no CRCMG.

ESPECIFICAÇÕES INDIVIDUALIZADAS

FIREWALL DA PRÓXIMA GERAÇÃO - NEXT-GENERATION FIREWALL (NGFW)

REQUISITOS MÍNIMOS DE FUNCIONALIDADE

5.22. Para a perfeita execução dos serviços, a Contratada deverá disponibilizar os materiais, equipamentos, ferramentas e utensílios necessários, nas quantidades estimadas e qualidades a seguir estabelecidas, promovendo sua substituição quando necessário:

ESPECIFICAÇÃO:

5.23. Deverá ser fornecido equipamento de Firewall de Próxima Geração (*Next-Generation Firewall*) como serviço contendo as seguintes especificações mínimas:

5.23.1. Mínimo de 2 slots para 10 Gigabit Ethernet SFP+.

5.23.2. Mínimo de 8 portas Gigabit Ethernet RJ-45 para conexão LAN ou WAN.

5.23.3. Deverá possuir porta de console RJ-45 e porta de gerenciamento USB.

5.23.4. Throughput de, no mínimo, 25 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, com tamanho do pacote de 1518 bytes.

5.23.5. Throughput de, no mínimo, 4,5 Gbps de análise IPS.

5.23.6. Suporte a, no mínimo, 3 milhões de sessões TCP concorrentes.

5.23.7. Suporte a, no mínimo, 124.000 novas sessões TCP por segundo.

5.23.8. Throughput de, no mínimo, 25Gbps em VPN IPSec considerando pacote de tamanho 512 byte.

5.23.9. Throughput de, no mínimo, 1,4Gbps em VPN SSL ou IPSec.

5.23.10. Suporte a, no mínimo, 200 usuários concorrentes em VPN SSL ou IPSec.

5.23.11. Throughput de, no mínimo, 2,5Gbps de inspeção IPS em SSL ou IPSec.

5.23.12. Suporte a tensão de entrada em 110V ou 220V.

Características Gerais

5.24. A solução deve consistir em plataforma de proteção de rede baseada em appliance com todas as funcionalidades de Next Generation Firewall (NGFW) habilitadas sem limite de licenciamento, seja por funcionalidade, seja por quantidade;

5.25. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

5.26. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;

5.27. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

5.28. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

5.29. A gestão do equipamento deve ser compatível através da interface de gestão Web no mesmo dispositivo de proteção da rede;

5.30. Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q;

5.31. Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP;

5.32. Os dispositivos de proteção de rede devem possuir suporte a *Policy based routing* ou *policy based forwarding*;

5.33. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

5.34. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;

5.35. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;

5.36. Os dispositivos de proteção de rede devem suportar sFlow;

5.37. Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;

5.38. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;

5.39. Deve suportar NAT dinâmico (Many-to-1);

5.40. Deve suportar NAT dinâmico (*Many-to-Many)*;

5.41. Deve suportar NAT estático (1-to-1);

5.42. Deve suportar NAT estático (*Many-to-Many*);

5.43. Deve suportar NAT estático bidirecional 1-to-1;

5.44. Deve suportar Tradução de porta (PAT);

5.45. Deve suportar NAT de Origem;

5.46. Deve suportar NAT de Destino;

5.47. Deve suportar NAT de Origem e NAT de Destino simultaneamente;

5.48. Deve poder combinar NAT de origem e NAT de destino na mesma política.

5.49. Deve implementar *Network Prefix Translation* (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

5.50. Deve suportar NAT64 e NAT46;

5.51. Deve implementar o protocolo ECMP;

5.52. Deve implementar balanceamento de link por hash do IP de origem;

5.53. Deve implementar balanceamento de link por hash do IP de origem e destino;

5.54. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;

5.55. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;

5.56. Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;

5.57. Enviar log para sistemas de monitoração externos, simultaneamente;

5.58. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;

5.59. Proteção anti-spoofing;

5.60. Implementar otimização do tráfego entre dois equipamentos do mesmo fabricante;

5.61. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

5.62. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

5.63. Suportar OSPF graceful restart;

5.64. Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);

5.65. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

5.66. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;

5.67. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;

5.68. Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

5.69. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;

5.70. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3;

5.71. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster;

5.72. A configuração em alta disponibilidade deve sincronizar: Sessões;

5.73. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;

5.74. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;

5.75. A configuração em alta disponibilidade deve sincronizar:Tabelas FIB;

5.76. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;

5.77. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;

5.78. Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo-ativo ou ativo-passivo, permitindo a distribuição de carga entre diferentes contextos;

5.79. Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;

5.80. O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado a, exportar configuração dos sistemas virtuais (contextos) por ambas interfaces;

5.81. Controle, inspeção e descriptografia de SSL para tráfego de entrada (Inbound) e saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);

5.82. Deve apoiar um tecido de segurança para fornecer uma solução de segurança holística abrangendo toda a rede;

5.83. O tecido de segurança deve identificar potenciais vulnerabilidades e destacar as melhores práticas que poderiam ser usadas para melhorar a segurança e o desempenho geral de uma rede;

5.84. Deve existir um Serviço de Suporte que ofereça aos clientes uma verificação de saúde recorrente com um relatório de auditoria mensal personalizado de seus appliances NGFW;

Controle por Política de Firewall

5.85. Deverá suportar controles por zona de segurança;

5.86. Controles de políticas por porta e protocolo;

5.87. Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;

5.88. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

5.89. Firewall deve ser capaz de aplicar a inspeção UTM (Application Control e Webfiltering no mínimo) diretamente às políticas de segurança versus via perfis;

5.90. Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados diretamente às políticas de firewall;

5.91. Deve suportar o armazenamento de logs em tempo real tanto para o ambiente de nuvem quanto o ambiente local (on-premise);

5.92. Deve suportar o padrão de indústria *'syslog' protocol* para armazenamento usando o formato Common Event Format (CEF);

5.93. Deve haver uma maneira de assegurar que o armazenamento dos logs em tempo real não supere a velocidade de upload;

5.94. Deve suportar o protocolo padrão da indústria VXLAN;

Controle de Aplicações

5.95. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

5.96. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

5.97. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

5.98. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

5.99. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

5.100. Deve detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Bittorrent e aplicações VOIP que utilizam criptografia proprietária;

5.101. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;

5.102. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

5.103. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex;

5.104. Identificar o uso de táticas evasivas via comunicações criptografadas;

5.105. Atualizar a base de assinaturas de aplicações automaticamente;

5.106. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;

5.107. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory na versão instalada atualmente, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

5.108. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

5.109. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

5.110. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

5.111. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;

5.112. A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, RTSP e SSL;

5.113. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

5.114. Deve alertar o usuário quando uma aplicação for bloqueada;

5.115. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;

5.116. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;

5.117. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;

5.118. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;

5.119. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);

5.120. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;

5.121. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;

5.122. Deve ser possível configurar Application Override permitindo selecionar aplicações individualmente.

Prevenção de Ameaças

5.123. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

5.124. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

5.125. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

5.126. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

5.127. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;

5.128. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

5.129. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

5.130. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

5.131. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

5.132. Deve permitir o bloqueio de vulnerabilidades;

5.133. Deve permitir o bloqueio de exploits conhecidos;

5.134. Deve incluir proteção contra-ataques de negação de serviços;

5.135. Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise de padrões de estado de conexões;

5.136. Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise de decodificação de protocolo;

5.137. Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise para detecção de anomalias de protocolo;

5.138. Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise heurística;

5.139. Deverá possuir o seguinte mecanismo de inspeção de IPS: IP Defragmentation;

5.140. Deverá possuir o seguinte mecanismo de inspeção de IPS: Remontagem de pacotes de TCP;

5.141. Deverá possuir o seguinte mecanismo de inspeção de IPS: Bloqueio de pacotes malformados;

5.142. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;

5.143. Detectar e bloquear a origem de portscans;

5.144. Bloquear ataques efetuados por worms conhecidos;

5.145. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

5.146. Possuir assinaturas para bloqueio de ataques de buffer overflow;

5.147. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

5.148. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

5.149. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

5.150. Suportar bloqueio de arquivos por tipo;

5.151. Identificar e bloquear comunicação com botnets;

5.152. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

5.153. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;

5.154. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;

5.155. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;

5.156. Os eventos devem identificar o país de onde partiu a ameaça;

CRCMG
CONSELHO REGIONAL DE CONTABILIDADE
DE MINAS GERAIS

5.157. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

5.158. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

5.159. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança etc., ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;

5.160. O Firewall deve permitir que se analise a implantação de Tecido de Segurança para identificar potenciais vulnerabilidades e destaque as práticas recomendadas que podem ser usadas para melhorar a segurança e o desempenho geral da rede;

5.161. Caso o firewall possa ser coordenado por software de segurança do computador do usuário final (laptop, desktop etc.) deve ter um perfil onde se possa executar a análise de vulnerabilidade nestes equipamentos de usuário e assegurar que estes executem versões compatíveis;

5.162. Análise de postura de segurança devem existir para permitir que o software de segurança do endpoint aplique proteção em tempo real, antivírus, filtragem da Web e controle de aplicativos no endpoint;

5.163. Fornecem proteção contra-ataques de dia zero por meio de estreita integração com os componentes Security Fabric, incluindo NGFW, Sandbox (on-premise e nuvem);

Filtro de URL

5.164. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

5.165. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

5.166. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

5.167. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local, em modo de proxy transparente e explícito;

5.168. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

5.169. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;

5.170. Possuir pelo menos 60 categorias de URLs;

5.171. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;

5.172. Permitir a customização de página de bloqueio;

5.173. Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);

5.174. Além do Explicit Web Proxy, suportar proxy Web transparente;

Identificação de Usuários

5.175. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;

5.176. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

5.177. Deve possuir integração e suporte a Microsoft Active Directory para os seguintes sistemas operacionais: Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 e Windows Server 2012 R2;

5.178. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado, a utilização de sistemas virtuais, segmentos de rede, etc;

5.179. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

5.180. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

5.181. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

5.182. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

5.183. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

5.184. Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução;

5.185. Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator;

QoS e Traffic Shaping

5.186. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube, Ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;

5.187. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;

5.188. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;

5.189. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;

5.190. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

5.191. Suportar a criação de políticas de QoS e Traffic Shaping por porta;

5.192. O QoS deve possibilitar a definição de tráfego com banda garantida;

5.193. O QoS deve possibilitar a definição de tráfego com banda máxima;

5.194. O QoS deve possibilitar a definição de fila de prioridade;

5.195. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;

5.196. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

5.197. Suportar modificação de valores DSCP para o Diffserv;

5.198. Suportar priorização de tráfego usando informação de Type of Service;

5.199. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;

5.200. Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes;

Filtro de Dados

5.201. Permitir a criação de filtros para arquivos e dados pré-definidos;

5.202. Os arquivos devem ser identificados por extensão e tipo;

5.203. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);

5.204. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

5.205. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

5.206. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;

Geolocalização

5.207. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

5.208. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

5.209. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;

VPN

5.210. Suportar VPN Site-to-Site e Cliente-To-Site;

5.211. Suportar IPSec VPN;

5.212. A VPN IPSEc deve suportar 3DES;

5.213. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;

5.214. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

5.215. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

5.216. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);

5.217. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI;

5.218. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

5.219. Suportar VPN em em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;

5.220. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;

5.221. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;

5.222. Atribuição de DNS nos clientes remotos de VPN;

5.223. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN;

5.224. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;

5.225. Suportar leitura e verificação de CRL (certificate revocation list);

5.226. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

5.227. Deve permitir que a conexão com a VPN seja estabelecida da seguinte forma: Antes do usuário autenticar na estação;

5.228. Deve permitir que a conexão com a VPN seja estabelecida da seguinte forma: Após autenticação do usuário na estação;

5.229. Deve permitir que a conexão com a VPN seja estabelecida da seguinte forma: Sob demanda do usuário;

5.230. Deverá manter uma conexão segura com o portal durante a sessão;

5.231. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);

Wireless Controller

5.232. Deve ser capaz de gerenciar de maneira centralizada outros pontos de acesso do mesmo fabricante;

5.233. Suporte ao serviço de servidor DHCP por SSID para prover endereçamento IP automático para os clientes wireless;

5.234. Suportar IPv4 e IPv6 por SSID;

5.235. Permitir escolher se o tráfego de cada SSID será enviado à controladora ou comutado diretamente pela interface do ponto de acesso em determinada VLAN;

5.236. Permitir definir quais redes serão acessadas através da controladora e quais redes serão comutadas diretamente pela interface do ponto de acesso;

5.237. Suporte a monitoração e supressão de ponto de acesso indevido;

5.238. Prover autenticação para a rede wireless através de bases externas como LDAP ou RADIUS;

5.239. Permitir autenticar usuários da rede wireless de forma transparente em domínio Windows;

5.240. Deverá permitir a visualização dos clientes wireless conectados por usuário;

5.241. Deverá permitir a visualização dos clientes wireless conectados por IP;

5.242. Deverá permitir a visualização dos clientes wireless conectados por tipo de autenticação;

5.243. Deverá permitir a visualização dos clientes wireless conectados por canal;

5.244. Deverá permitir a visualização dos clientes wireless conectados por largura de banda utilizada;

5.245. Deverá permitir a visualização dos clientes wireless conectados por potência do sinal;

5.246. Deverá permitir a visualização dos clientes wireless conectados tempo de conexão;

5.247. Deverá prover suporte a Fast Roaming em autenticação com Captive Portal;

5.248. Deve suportar configuração de Captive Portal por SSID;

5.249. Permitir configurar o bloqueio de tráfego entre os clientes conectados a um SSID e AP específico;

5.250. Ser compatível com Wi-Fi Protected Access (WPA) e WPA2 por SSID, utilizando-se de algorítmo AES e/ou TKIP;

5.251. Deverá suportar 802.1x através de RADIUS na controladora wireless;

5.252. Permitir configurar parâmetros de rádio, como banda e canal, na controladora wireless;

5.253. A controladora deve possuir método de descoberta de novos Pontos de Acesso de maneira automática;

5.254. A controladora deve possuir método de descoberta de novos Pontos de Acesso baseados em IP estático;

5.255. A controladora deve possuir método de descoberta de novos Pontos de Acesso baseados em DHCP;

5.256. A controladora deve possuir método de descoberta de novos Pontos de Acesso por DNS;

5.257. A controladora deve possuir método de descoberta de novos Pontos de Acesso baseados em Broadcast;

5.258. A controladora deve possuir método de descoberta de novos Pontos de Acesso baseados em Multicast;

5.259. A controladora deve fornecer lista contendo Pontos de Acesso autorizados e Pontos de Acesso indevidos (Rogue);

5.260. Possuir proteção contra-ataques do tipo ARP Poisoning na controladora wireless;

5.261. Implementar Protected Management Frames de acordo com a norma da aliança WiFi e o padrão 802.11ac;

5.262. Possuir WIDS integrado com detecção de ataques ASLEAP;

5.263. Possuir WIDS integrado com detecção de ataques do tipo Association Frame Flooding;

5.264. Possuir WIDS integrado com detecção de ataques de authentication Frame Flooding;

5.265. Possuir WIDS integrado com detecção de ataques de Broadcast De-authentication;

5.266. Possuir WIDS integrado com detecção de ataques de EAPOL Packet flooding;

5.267. Possuir WIDS integrado com detecção de ataques de Invalid MAC OUI;

5.268. Possuir WIDS integrado com detecção de ataques de Long Duration Attack;

5.269. Possuir WIDS integrado com detecção de ataques de Null SSID probe response;

5.270. Possuir WIDS integrado com detecção de ataques de Spoofed De-authentication;

5.271. Possuir WIDS integrado com detecção de ataques de Weak WEP IV Detection;

5.272. Possuir WIDS integrado com detecção de ataques de Wireless Bridge;

5.273. Implementar canais de aprovisionamento automático dos Access Points, de forma a minimizar interferência entre eles;

5.274. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;

5.275. Permitir definir em quais horários determinados SSID estará disponível;

5.276. A controladora wireless deverá oferecer Firewall integrado UTM, baseado em identidade do usuário;

5.277. Possibilitar definir número máximo de clientes permitidos por SSID;

5.278. Possibilitar definir número máximo de clientes permitidos por AP;

5.279. Possibilitar definir número máximo de clientes permitidos por Radio;

5.280. Deve permitir criar, gerenciar e disponibilizar redes wireless mesh;

5.281. Possuir mecanismo de criação automática e/ou manual de usuários visitantes e senhas, que possam ser enviadas por email ou SMS aos usuários, e com ajuste de tempo de expiração da senha;

5.282. A comunicação entre o ponto de acesso e a controladora wireless deve poder ser efetuada de forma criptografada usando o protocolo DTLS;

5.283. Deve possuir mecanismo de ajuste de potência do sinal de forma a reduzir interferência entre canais entre dois pontos de acesso gerenciados;

5.284. Possuir mecanismo de balanceamento de tráfego/usuários entre pontos de acesso;

5.285. Possuir mecanismo de balanceamento de tráfego/usuários entre frequências e/ou radios dos pontos de acesso;

5.286. Deve permitir a identificação do firmware utilizado por cada pontos de acesso gerenciado e permitir a atualização via interface gráfica;

5.287. Permitir que sejam desabilitados clientes wireless que possuam taxa de transmissão baixa;

5.288. Permitir bloquear clientes wireless que tenham sinal fraco, definindo um limiar de sinal a partir do qual tais clientes serão ignorados;

5.289. Deve permitir configurar o valor de Short Guard Interval para 802.11n e 802.11ac em 5GHz;

5.290. Deve permitir selecionar individualmente em cada pontos de acesso quais os SSIDs que serão propagados;

5.291. Deve permitir associação dinâmica de VLANs aos usuários autenticados via RADIUS num SSID

5.292. Deve permitir associação dinâmica de VLANs aos usuários autenticados via vlan pooling;

5.293. Deve permitir visualizar as aplicações e ameaças por dispositivo wireless;

5.294. Deve permitir identificar os clientes wifi que apresentem algum risco baseado em aplicações;

5.295. Deve permitir identificar os clientes wifi que apresentem algum risco baseado em endereço de destino;

5.296. Deve permitir identificar os clientes wifi que apresentem algum risco baseado em ameaças;

5.297. Deve permitir identificar os clientes wifi que apresentem algum risco baseado em sessões;

5.298. A controladora wireless deve suportar uma licença que permita pelo menos 10000 assinaturas de aplicações para reconhecimento do tráfego;

5.299. A controladora wireless deve possuir interface de gerência integrada no próprio equipamento;

5.300. A controladora wireless deve possuir a funcionalidade de Fast-de roaming para aos enlaces mesh entre os nós secundários e principais;

5.301. A controladora wireless deve suportar aceleração de tráfego do protocolo CAPWAP através de um processador de rede específico para a função;

5.302. A controladora wireless deve suportar aceleração de encapsulamento de túnel de tráfego de bridge wireless através de um processador de rede específico para a função;

5.303. A controladora wireless deve suportar protocolo LLDP;

5.304. Deve permitir técnica de detecção de APs intrusos On-wire através de endereço MAC exato;

5.305. Deve permitir técnica de detecção de APs intrusos On-wire através de endereço MAC adjacente;

5.306. Deve permitir a visualização dos usuários conectados em forma de topologia lógica de rede representando a quantidade de dados transmitidos e recebidos;

5.307. A controladora wireless deve permitir combinar redes WiFi e redes cabeadas con um software switch integrado;

5.308. A controladora wireless deve permitir criar um captive portal no software switch integrado para redes WiFi e redes cabeadas;

5.309. A controladora wireless deve permitir gerenciar switches de acesso do mesmo fabricante da solução ofertada;

5.310. Deverá suportar a conversão de Multicast a Unicast para melhorar o rendimento do airtime;

5.311. No ambiente de alta disponibilidade, deve existir a função dos controladores wireless primário e secundário na unidade AP, permitindo que a unidade decida a ordem em que o AP seleciona uma unidade controladora e como a unidade AP conecta à unidade controladora backup se a controladora primária falhar;

5.312. Deve fornecer capacidade para criar várias chaves pré-compartilhadas de acesso protegido WiFi (WPA-PSKs) para que o compartilhamento de PSK entre dispositivos não seja necessário;

Especificação de plataforma multifator de autenticação (Quantidade: 100 usuários) - firewall:

5.313. Funcionalidades:

5.313.1. A plataforma multifator de autenticação deverá ser do mesmo fabricante do ITEM 1.

5.313.2. A modalidade de licenciamento deverá ser perpétua.

5.313.3. A plataforma multifator de autenticação deverá ser uma aplicação geradora de OTP (One Time Password) suportando tanto tokens baseados em tempo (TOTP) quanto baseados em eventos (HOTP).

5.313.4. A aplicação deverá ser disponibilizada para dispositivos com sistemas operacionais Android, iOS e Windows Mobile.

5.313.5. Os seeds de token deverão ser gerados dinamicamente, minimizando exposição online, e os seeds deverão ser sempre criptografados em repouso ou em movimento.

5.313.6. Os detalhes de login devem ser enviados via push para os telefones com o aplicativo para aprovação em um único toque.

5.313.7. A aplicação deve ser protegida por PIN/Fingerprinting.

5.313.8. Deverá ser possível copiar a OTP para a área de transferência do dispositivo na qual está instalada a aplicação.

5.313.9. A aplicação deverá ter proteção contra auto apagamento por força bruta.

5.313.10. A aplicação deverá possuir compatibilidade com Apple watch.

PLATAFORMA DE ZERO TRUST (CONFIANÇA ZERO) PARA O MÍNIMO DE 100 USUÁRIOS

REQUISITOS MÍNIMOS DE FUNCIONALIDADE

5.314. Para a perfeita execução dos serviços, a Contratada deverá disponibilizar os materiais, equipamentos, ferramentas e utensílios necessários, nas quantidades estimadas e qualidades a seguir estabelecidas, promovendo sua substituição quando necessário:

ESPECIFICAÇÃO:

5.315. Funcionalidades:

5.315.1. A plataforma de *Zero Trust* deve ser do mesmo fabricante do item 1 a fim de proporcionar a melhor integração, funcionalidade, suporte e garantia de evolução.

5.315.2. O fornecedor deverá fornecer infraestrutura necessária em nuvem própria ou nuvem pública, sem ônus para o CRCMG, para o adequado funcionamento de toda a solução de gerenciamento.

5.315.3. Deve prover método de controle de acesso que utilize identificação de dispositivo cliente, autenticação e *tags* de postura de segurança para fornecer acesso a aplicações baseado em perfis.

5.315.4. O acesso às aplicações deve ser garantido somente após a verificação do dispositivo, autenticação da identidade do usuário, autorização do usuário e avaliação de postura baseada em contexto, utilizando *tags* de postura de segurança.

5.315.5. Deve prover um *gateway* de aplicações que permita aos usuários acessarem localmente e remotamente recursos por meio de um *proxy* de acesso criptografado por SSL, de modo que essa tecnologia de acesso remoto elimine a necessidade de uso de VPN (*Virtual Private Network*).

5.315.6. Deve fornecer controle de acesso baseado em IP/MAC que combine essas informações com *tags* de postura para identificação e avaliação de postura de segurança e implementar acesso *zero trust* baseado em perfil.

5.315.7. Deve fornecer plataforma que aja como Certificate Authority (CA) de *zero trust*, fornecendo certificados de clientes para clientes que façam tais requisições, aplicando *tags* de segurança de acordo com as regras de *zero trust* previamente configuradas.

5.315.8. O *gateway* de aplicações deve realizar proxy de protocolos HTTP, SSH, RDP, SMB, FTP, e tráfego TCP sobre conexões seguras estabelecidas com o cliente.

5.315.9. O *proxy* de acesso deverá utilizar HTTPS e agir com o *proxy* reverso para o servidor HTTP, de modo o cliente, ao conectar-se com uma página *web* hospedada pelo servidor protegido, o endereço seja resolvido para o endereço IP do *proxy* de acesso, sejam tomadas ações para autenticar o usuário utilizando o certificado presente no navegador e seja verificado junto ao registro de dispositivo existente na plataforma de *zero trust*.

5.315.10. O *proxy* de acesso para encaminhamento de tráfego TCP deve trabalhar como *proxy* reverso HTTPS, realizando túnel deste tráfego entre o cliente e o *proxy* de acesso sobre HTTPS, e encaminhá-lo ao recurso protegido.

5.315.11. O *proxy* de encaminhamento TCP deve suportar verificação (*scanning*) de ameaças e inspeção profunda (*deep inspection*) para protocolos HTTP, HTTPS, SMTP, SMTPS, IMAP, IMAPS, POP3, POP2S, SMB e CIFS.

5.315.12. Deve realizar, no mínimo, a verificação de postura de dispositivos quanto a:

5.315.13. Dispositivos vulneráveis, classificados de acordo com o risco identificado.

5.315.14. Presença e funcionamento de algum software antivírus.

5.315.15. Atualização da assinatura (base de dados) de antivírus.

5.315.16. Se o software Windows Defender está habilitado (para dispositivos utilizando sistema operacional Microsoft Windows).

5.315.17. Se a criptografia de disco Microsoft Bitlocker está habilitada (para dispositivos utilizando sistema operacional Microsoft Windows) ou se o FileVault Disk Encryption está habilitado (para dispositivos utilizando sistema operacional macOS).

5.315.18. Se a funcionalidade Exploit Guard da Microsoft está habilitada (para dispositivos utilizando sistema operacional Microsoft Windows).

5.315.19. Se a funcionalidade Application Guard da Microsoft está habilitada (para dispositivos utilizando sistema operacional Microsoft Windows).

5.315.20. Se o firewall do Windows está habilitado (para dispositivos utilizando sistema operacional Microsoft Windows).

5.315.21. Se o aplicativo cliente da plataforma para funcionamento da plataforma *zero trust* está instalada e a telemetria está conectada.

5.315.22. Presença de vulnerabilidades conhecidas com base no padrão CVE (*Common Vulnerabilitues and Exposures*).

5.315.23. Se o dispositivo Microsoft Windows ou Apple macOS é membro de um domínio Microsoft.

5.315.24. Se há a presença de determinado arquivo e dispositivos Windows, macOS ou Linux.

5.315.25. Se há a presença de determinada chave de registro no Registro de dispositivos Microsoft Windows.

5.315.26. Se há a presença de determinado processo rodando em dispositivos Microsoft Windows, Apple macOS ou Linux.

PLATAFORMA DE GERENCIAMENTO, MONITORAMENTO E ARMAZENAMENTO DE LOGS

REQUISITOS MÍNIMOS DE FUNCIONALIDADE

5.316. Para a perfeita execução dos serviços, a Contratada deverá disponibilizar os materiais, equipamentos, ferramentas e utensílios necessários, nas quantidades estimadas e qualidades a seguir estabelecidas, promovendo sua substituição quando necessário:

ESPECIFICAÇÃO:

5.317. Funcionalidades

5.317.1. A plataforma de gerenciamento, monitoramento e armazenamento de logs deve ser do mesmo fabricante do item 1 a fim de proporcionar a melhor integração, funcionalidade, suporte e garantia de evolução.

5.317.2. Deve poder coletar logs do equipamento objeto da presente contratação conforme disposto no Item 1 incluindo, no mínimo, os seguintes logs de segurança: antivírus, Intrusion Prevention, Application Control, Web Filter, File Filter, DNS, Data Leak Prevention, Email Filter, Web Application Firewall, Vulnerability Scan e VoIP.

5.317.3. Deverá possuir painel centralizado fornecendo *widgets* de monitoramento em tempo real do sistema e de logs.

5.317.4. Deverá possuir filtros de logs e a capacidade de realização de download destes logs.

5.317.5. Deverá permitir análise em tempo real de atividade de rede, de usuários e perfis de alertas.

5.317.6. Deverá permitir a geração de relatórios personalizáveis e agendamentos de relatórios em diferentes formatos.

5.317.7. Deverá permitir backup agendado de configurações dos firewalls gerenciados, bem como gerenciamento de scripts a serem executados remotamente nestes dispositivos.

5.317.8. Deverá permitir que acesse a configuração do dispositivo pelo navegador da web, modifique sua configuração e envie as alterações para o dispositivo por meio da rede.

5.317.9. Deverá permitir a configuração de alertas por e-mail para emergências específicas da estrutura da rede.

5.317.10. Deverá possibilitar a listagem das maiores ameaças identificadas no firewall gerenciado contendo, no mínimo:

5.317.11. Aplicações em risco detectadas pelo controle de aplicações.

5.317.12. Incidentes de intrusões detectadas pelo IPS (*Intrusion Prevention System*).

5.317.13. Malware/botnets identificados pelo sistema de antivírus.

5.317.14. Incidentes de DLP (*Data Loss Prevention*).

5.317.15. Anomalias de rede.

5.317.16. Deverá possibilitar a identificação das seguintes informações na análise de tráfego do firewall gerenciado:

5.317.17. Exibir os principais aplicativos usados na rede, incluindo o nome do aplicativo, a categoria, a largura de banda (enviada/recebida), as sessões e o nível de risco.

5.317.18. Exibir os principais aplicativos de nuvem usados na rede.

5.317.19. Exibir o tráfego de rede mais alto por endereço IP e nome de origem, largura de banda (enviada/recebida), sessões e nível de risco.

5.317.20. Exibir o maior tráfego de rede por usuário em termos de largura de banda enviada/recebida, sessões e nível de risco.

5.317.21. Exibir o tráfego de rede mais alto por endereços IP de destino, os aplicativos usados para acessar o destino, a largura de banda enviada/recebida, as sessões e o nível de risco.

5.317.22. Exibir o tráfego de rede mais alto por interface em termos de largura de banda enviada/recebida, sessões de tráfego e nível de risco – tanto por interface de origem quanto por interface de destino.

5.317.23. Exibir o maior tráfego de rede por país em termos de largura de banda enviada/recebida, sessões de tráfego e nível de risco – Tanto por país de origem ou de destino.

5.317.24. Exibir os principais domínios de sites permitidos e bloqueados na rede.

5.317.25. Exibir os principais usuários de navegação na Web e seus endereços IP por duração total do tempo de navegação.

5.317.26. Exibir eventos nos dispositivos gerenciados, sua gravidade e o número de incidentes.

5.317.27. Exibir os usuários que efetuaram login nos dispositivos gerenciados, o número de alterações de configuração que realizaram, o número de sessões de administração e a duração total do tempo de login.

5.317.28. Exibir os usuários que não conseguiram fazer login nos dispositivos gerenciados.

5.317.29. Exibir os nomes dos túneis VPN com IPsec que estão acessando a rede.

5.317.30. Exibir os usuários que estão acessando a rede usando um túnel VPN SSL ou IPsec.

5.317.31. Deverá permitir a exportação de todos estes dados para arquivo em formato CSV.

5.317.32. A plataforma deverá ser fornecida na modalidade de plataforma como serviço em nuvem do próprio fornecedor ou nuvem pública, sem custos adicionais de hospedagem, tráfego de dados ou processamento.

5.317.33. Deverá armazenar 1 ano de logs.

SERVIÇOS PROFISSIONAIS DE IMPLEMENTAÇÃO DA SOLUÇÃO

Especificação de serviços profissionais de implementação da solução:

PARA O FIREWALL DE PRÓXIMA GERAÇÃO:

5.318. Instalação do equipamento em rack padrão 19" do CRCMG ou em bandeja destinada a essa finalidade.

5.319. Configuração de parâmetros de rede e conectividade.

5.320. Integração do Firewall com o Active Directory do CRCMG para autenticação integrada.

5.321. Configuração de redundância e balanceamento de carga entre links.

5.322. Configuração da funcionalidade de UTM (*Unified Threat Management*) para *web filter* e controle de aplicações.

5.323. Configuração de IPS/IDS.

5.324. Configuração do antivírus de borda.

5.325. Configuração das regras de firewall aplicáveis às necessidades do CRCMG.

5.326. Configuração do serviço de atualização de bases de dados de vacinas de antivírus, IPS/IDS e outras disponíveis.

5.327. Configuração do sistema de armazenamento de logs do equipamento.

PARA O SISTEMA DE ZERO TRUST:

5.328. Instalação e parametrização do sistema de gerenciamento Zero Trust em infraestrutura necessária em nuvem própria ou nuvem pública, sem ônus para o CRCMG, para o adequado funcionamento de toda a solução de gerenciamento.

5.329. Parametrização da plataforma para registro dos usuários do CRCMG.

5.330. Parametrização da plataforma para integração com o Microsoft Active Directory existente no CRCMG.

5.331. Parametrização da plataforma para realizar a conexão aos recursos (aplicações) do CRCMG em substituição à tecnologia de VPN tradicional.

5.332. Parametrização de políticas de verificação de postura de segurança e regras de conexão *Zero Trust* de acordo com as funcionalidades existentes e aplicáveis ao ambiente do CRCMG.

PARA A PLATAFORMA DE GERENCIAMENTO, MONITORAMENTO E ARMAZENAMENTO DE LOGS:

5.333. Instalação e parametrização da plataforma a fim de gerenciar, monitorar e armazenar os logs do firewall gerenciado pelo período mínimo de 1 ano.

5.334. Elaborar, no mínimo, 5 tipos de relatórios a serem solicitados pelo CRCMG e deixar sua geração agendada para envio mensal.

PARA A PLATAFORMA DE MULTIFATOR DE AUTENTICAÇÃO:

5.335. Disponibilização das licenças de uso para atribuição aos usuários do CRCMG a ser realizada exclusivamente pela CONTRATADA, de acordo com as necessidades informadas pela CONTRATANTE. A CONTRATANTE não será responsável pela execução ou gestão deste processo.

OPERAÇÃO ASSISTIDA;

5.336. Operação assistida:

5.336.1. O ambiente deverá contar com operação assistida por até uma semana após o Go Live do projeto.

5.336.2. A operação assistida poderá ser remota para o acompanhamento de logs de erros e desempenho, porém deverá contar com o deslocamento de um consultor para o CRCMG caso haja algum problema na operação do ambiente.

5.337. Documentação

5.337.1. A documentação completa do projeto deverá ser entregue em até 15 (quinze) dias após a finalização da operação assistida.

5.337.2. A documentação deverá conter todos os itens parametrizados (IPs, usuários, senhas, etc) de maneira clara para futuras consultas.

SERVIÇOS PROFISSIONAIS DE SUPORTE TÉCNICO EM TODA SOLUÇÃO

5.338. RESPONSABILIDADE EXCLUSIVA PELA REALIZAÇÃO DOS SERVIÇOS:

5.338.1. Todos os serviços contratados são de realização exclusiva da CONTRATADA, incluindo a implementação, operação, gerenciamento e manutenção do firewall e das plataformas associadas. A CONTRATANTE terá acesso ao Firewall apenas para consulta e à plataforma de gerenciamento, monitoramento e armazenamento de logs, com a finalidade de criação e/ou geração de relatórios. Nenhum contato com a fabricante será de responsabilidade da CONTRATANTE, sendo essa atribuição exclusiva da CONTRATADA.

5.338.2. A empresa contratada deve implementar medidas de segurança da informação compatíveis com as melhores práticas do mercado e normas internacionais, como a ISO/IEC 27001 (Sistema de Gestão de Segurança da Informação), para garantir a proteção contra ameaças cibernéticas, acessos não autorizados e vazamentos de dados.

5.338.3. Todos os dados em trânsito (informações transmitidas entre sistemas) e em repouso (dados armazenados nos dispositivos e logs) devem ser protegidos por criptografia robusta, seguindo padrões internacionais como AES-256 ou equivalentes.

ESCOPO DE SERVIÇOS CONTINUADOS PRESTADOS PELA CONTRATADA

5.339. Após a instalação a CONTRATADA deverá manter, monitorar e gerenciar todo o ambiente após a sua instalação na modalidade 8x5;

5.340. Efetuar toda rotina de backup das configurações semanalmente;

5.341. Atualizar todos os equipamentos sempre que a versão de software, disponibilizada pelo fabricante, for considerada estável, negociando com a CONTRATANTE janelas de manutenção para efetuar o procedimento;

5.342. Realizar as seguintes configurações sempre que solicitadas pela CONTRATANTE:

5.343. Atividades relativas à Solução de Segurança:

5.343.1. Criação das rotas para links.

5.343.2. Criação de NAT.

5.343.3. Liberação de portas.

5.343.4. Configuração do Filtro de Conteúdo.

5.343.5. Configuração do Controle de Aplicativos.

5.343.6. Configuração do Agente para autenticação LDAP.

5.343.7. Configuração para o Single Sign-On (SSO).

5.343.8. Configurações dos serviços avançados de segurança (IPS, Antivírus).

5.343.9. Configuração de VPN client to site

5.343.10. Configuração de VPN site to site

5.343.11. Criação de regras de Firewall.

5.343.12. Criação de regras de QoS.

5.343.13. Emitir relatório de segurança mensal por localidade.

5.343.14. Implementar o appliance de monitoramento e armazenamento de logs.

5.343.15. Criar relatórios e dashboards de acordo com as orientações a serem formuladas.

SLA DOS SERVIÇOS E ATENDIMENTO

5.344. Atuar proativamente na resolução de problemas relativos à parte lógica e física das soluções;

5.345. Deverá monitorar o ambiente a fim de garantir que os recursos estão funcionando adequadamente na solução;

5.346. Elaborar rotinas de backup das configurações do equipamento.

5.347. Gerar relatórios de acesso e desempenho da solução de firewall.

5.348. Deverá possuir sistema de abertura de chamados pela internet.

5.349. Monitor latência e *uptime* dos links configurados.

5.350. A CONTRATADA deve garantir os seguintes níveis de serviço e atendimento:

5.350.1. O tratamento dos chamados abertos junto à CONTRATADA visa à disponibilidade e à qualidade da operação do equipamento contratado. Para tanto, a CONTRATADA deverá garantir os atendimentos aos chamados dentro dos prazos e grau de severidade explicitados na tabela 2.

5.350.2. Para a realização de manutenções corretivas ou preventivas programadas, a CONTRATADA deverá planejar e negociar com a equipe de gestão de mudanças da CONTRATANTE, para obter a autorização do melhor período para as paralisações necessárias.

5.350.3. Para apuração do índice de tempo de atendimento para solução de problemas, os chamados são classificados em 4 (quatro) Níveis de Severidade, de acordo com a tabela 1, a seguir:

Níveis de Severidade	
1	Significa que seu ambiente de produção está desativado e não há nenhum workaround imediatamente disponível. O suporte de severidade 1 requer que o cliente tenha recursos dedicados disponíveis para trabalhar no problema de maneira contínua e possa ser encontrado durante as horas estabelecidas por esse contrato, ou seja, 8x5.
2	Ocorre quando uma funcionalidade importante está severamente prejudicada. As operações podem continuar de maneira restrita, embora a produtividade no longo prazo possa ser afetada. Um workaround temporário está disponível.
3	Envolve perda parcial, não crítica, do ambiente. Alguns componentes possuem operações prejudicadas, mas permite ao usuário continuar usando o ambiente. Mínimo risco do ambiente produtivo parar.
4	Refere-se a questões de uso geral. Questões de configurações habituais e problemas "cosméticos" e de otimização, não afetando em nada o ambiente.

Tabela 1 – Níveis de Severidade

5.351. Um chamado somente será considerado contingenciado ou concluído com o aceite da CONTRATANTE.

5.352. Para os chamados classificados como de **severidade 1** (um), a assistência técnica será prestada em regime 8x5 (on-site ou remota), com atendimento em até 2 (duas) horas úteis após o registro do chamado.

a) Em caso de adoção de uma solução de contingência ou de contorno, esta não poderá ser implementada em prazo superior a 8 (oito) horas úteis, após o registro do chamado.
b) Em sendo utilizada uma solução de contingência, a solução definitiva não poderá ultrapassar 3 (três) dias úteis após o registro do chamado, a não ser que envolva a troca do equipamento.

5.353. Para os chamados classificados como **severidade 2** (dois), a assistência técnica será prestada em regime 8x5 (remota ou on-site), com atendimento em até 4 (quatro) horas úteis após o registro do chamado.

a) Após a abertura de chamado, caso o problema não tenha sido contingenciado remotamente após 12 (doze) horas úteis, a assistência técnica deverá ser on-site e a solução de contingência ou de contorno não poderá ser implementada em prazo superior ao próximo dia útil, após o registro do chamado.
b) Em sendo utilizada uma solução de contingência ou contorno, a solução definitiva não poderá ultrapassar 8 (oito) dias úteis após o registro do chamado, a não ser que envolva a troca do equipamento.

5.354. Para os chamados classificados como **severidade 3** (três), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 16 (dezesseis) horas úteis após o registro do chamado.

a) A CONTRATADA terá, no máximo, 72 (setenta e duas) horas úteis, após o registro do chamado, para implantar uma solução definitiva ou de contingência.
b) Em sendo utilizada uma solução de contingência ou de contorno, a solução definitiva não poderá ultrapassar 30 (trinta) dias corridos após o registro do chamado, a não ser que envolva a troca do equipamento.

5.355. Para os chamados classificados como **severidade 4** (quatro), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 24 (vinte e quatro) horas úteis após o registro do chamado.

a) A CONTRATADA terá, no máximo, 15 dias corridos para responder ao chamado e solucionar, após o seu registro.
b) Não poderá haver limites no quantitativo de abertura de chamados.

5.356. Conceito: Disponibilidade da infraestrutura de firewall, incluindo hardware, licenças, software aplicações e demais recursos necessários para manter o serviço ativo e garantir a conectividade entre os serviços contratados, assegurando seu pleno funcionamento. Exceto a infraestrutura fornecida pela Contratante.

5.357. Nível mínimo de Serviço (SLA) acordado: 99,9% do tempo disponível, sendo este indicador medido mensalmente.

5.358. Os valores referentes aos períodos de interrupção mensal serão descontados na fatura do respectivo mês e será calculado conforme INSTRUMENTO DE MEDIÇÃO DE RESULTADO (IMR).

5.359. No caso de inoperância reincidente num período inferior a 03 (três) horas, contado a partir do restabelecimento do serviço da última inoperância, considerar-se-á como tempo de indisponibilidade do serviço o início da primeira inoperância até o final da última inoperância, quando o serviço estiver totalmente operacional.

5.360. Neste cálculo será considerado somente o tempo de indisponibilidade não previsto ou não planejado, reservando para posterior negociação períodos de manutenção preventiva ou corretiva que serão planejados com antecedência de no mínimo 72 horas.

Atendimento

5.361. Os serviços de suporte técnico especializado serão solicitados diretamente à contratada, mediante a abertura de chamado via sistema on-line, telefone ou e-mail.

5.362. É de responsabilidade da Contratada acionar fabricantes ou fornecedores para tratamento ou acompanhamento de incidentes, se for o caso.

5.363. Os prazos para solucionar os problemas objeto do chamado técnico estão definidos no item SLA dos serviços e atendimento.

5.364. O atendimento deverá ser prestado de segunda a sexta-feira no horário comercial do CRCMG, sendo das 8h30min às 17h30min.

5.365. A contratada deve possuir meios de receber registros de chamados fora do horário comercial do CRCMG, de forma que estes chamados comecem a ser contados a partir do próximo dia e hora útil.

REQUISITOS MÍNIMOS DE FUNCIONALIDADE RMA

5.366. Para a perfeita execução dos serviços, a Contratada deverá disponibilizar os materiais, equipamentos, ferramentas e utensílios necessários, nas quantidades estimadas e qualidades a seguir estabelecidas, promovendo sua substituição quando necessário:

Especificação de RMA do equipamento Firewall:

5.367. Para o Firewall de Próxima Geração:

5.367.1. Na eventualidade de falha de hardware do equipamento que o torne inoperante, um novo equipamento deverá ser entregue na sede do CRCMG em Belo Horizonte até 4 horas após o chamado aberto no fabricante, na modalidade 24x7, incluindo finais de semana ou feriados.

Responsabilidade da Contratada:

5.368. Todo o contato com o fabricante, incluindo a abertura do chamado, acompanhamento e resolução da falha de hardware, bem como os custos relacionados à substituição, transporte, entrega e quaisquer outros gastos adicionais decorrentes da falha, será de inteira responsabilidade da CONTRATADA e já deverão ser previstos na proposta. A CONTRATANTE não assumirá nenhuma responsabilidade por tais ações ou custos associados, cabendo exclusivamente à CONTRATADA garantir a execução do serviço conforme o prazo estipulado no item acima, sem prejuízo à operação da CONTRATANTE.

5.369. As demais ações de restauração dos serviços e funcionalidades no equipamento substituto seguirão o SLA disposto no "SLA DOS SERVIÇOS E ATENDIMENTO".

TREINAMENTO HANDS ON DA OPERAÇÃO DO AMBIENTE

Treinamento Hands On

5.370. Após a entrega da documentação deverá ser ministrado um treinamento hands on da operação do ambiente e deverá contemplar:

5.370.1. Utilização básica das ferramentas de gerenciamento dos equipamentos.

5.370.2. Orientação sobre criação de regras de firewall contendo inspeção UTM, IPS/IDS, antivírus de borda e demais funcionalidades de segurança aplicáveis.

5.370.3. Orientação sobre visualização de logs e indicadores relevantes para o monitoramento e gerenciamento do sistema de segurança da informação contida no Firewall de Próxima Geração.

5.370.4. Informações sobre troubleshooting inicial de problemas.

5.370.5. Informações sobre logs de sistema importantes para a operação do ambiente.

6. MODELO DE GESTÃO DO CONTRATO

6.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

6.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

6.3. As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

6.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

6.5. Após a assinatura do contrato ou instrumento equivalente, o órgão ou entidade poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

Preposto

6.6. A Contratada designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado.

6.7. A Contratante poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que a Contratada designará outro para o exercício da atividade.

Fiscalização

6.8. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput).

Fiscalização Técnica

6.9. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI);

6.10. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei nº 14.133, de 2021, art. 117, §1º e Decreto nº 11.246, de 2022, art. 22, II);

6.11. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. (Decreto nº 11.246, de 2022, art. 22, III);

6.12. O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. (Decreto nº 11.246, de 2022, art. 22, IV);

6.13. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato. (Decreto nº 11.246, de 2022, art. 22, V);

6.14. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou à prorrogação contratual (Decreto nº 11.246, de 2022, art. 22, VII).

Fiscalização Administrativa

6.15. O fiscal administrativo do contrato verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Art. 23, I e II, do Decreto nº 11.246, de 2022).

6.16. Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência; (Decreto nº 11.246, de 2022, art. 23, IV).

Gestor do Contrato

6.17. O gestor do contrato coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração. (Decreto nº 11.246, de 2022, art. 21, IV).

6.18. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. (Decreto nº 11.246, de 2022, art. 21, II).

6.19. O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III).

6.20. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. (Decreto nº 11.246, de 2022, art. 21, VIII).

6.21. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso. (Decreto nº 11.246, de 2022, art. 21, X).

6.22. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. (Decreto nº 11.246, de 2022, art. 21, VI).

6.23. O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

Da Confidencialidade

6.24. A propriedade dos dados e informações repassados ou gerados pela CONTRATANTE no ambiente provido pela CONTRATADA, por força do objeto desta licitação e do contrato, a qualquer momento, durante a vigência, término ou expiração do contrato, será exclusivamente da CONTRATANTE e constituem informação privilegiada e possuem natureza sigilosa, não podendo ser usadas por este fornecedor ou fornecidas a terceiros, sob nenhuma hipótese, sem autorização formal do contratante.

6.25. Os dados e informações do contratante devem residir exclusivamente em território nacional, incluindo replicação e cópias de segurança (backup), de modo que o contratante disponha de todas as garantias de legislação brasileira enquanto tomador do serviço e responsável pela guarda das informações armazenadas em nuvem.

Portabilidade e Transição Contratual

6.26. No encerramento do contrato, a solução deve estar disponível em prazo adequado e sem custo adicional, até a transferência completa para uma nova solução, de modo a garantir a continuidade do negócio e possibilitar a transição contratual.

6.27. No encerramento do contrato e após a formalização de pedido da CONTRATANTE, a CONTRATADA será responsável pela desativação, exclusão e limpeza de dados, metadados e configurações em ambiente fornecido para o serviço e em locais em que os dados do CRCMG foram armazenados, replicados ou espelhados, bem como pela retirada de equipamentos de sua propriedade ou de sua responsabilidade disponibilizados na sede da CONTRATADA.

7. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

7.1. A avaliação da execução do objeto utilizará o Instrumento de Medição de Resultado (IMR), conforme previsto no Anexo VII.

7.2. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

5.295.1.1. não produzir os resultados acordados,

5.295.1.2. deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas;

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

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

Do recebimento

7.4. Os serviços serão recebidos provisoriamente, no prazo de 5 (cinco) dias, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo. (Art. 140, I, a , da Lei nº 14.133, de 2021 e Arts. 22, X e 23, X do Decreto nº 11.246, de 2022).

7.5. O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda do contratado com a comprovação da prestação dos serviços a que se referem a parcela a ser paga.

7.6. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico. (Art. 22, X, Decreto nº 11.246, de 2022).

7.7. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo. (Art. 23, X, Decreto nº 11.246, de 2022).

7.8. O fiscal setorial do contrato, quando houver, realizará o recebimento provisório sob o ponto de vista técnico e administrativo.

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

7.10. Será considerado como ocorrido o recebimento provisório com a entrega do termo detalhado ou, em havendo mais de um a ser feito, com a entrega do último;

7.11. O Contratado fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição

de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

7.12. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório. (Art. 119 c/c art. 140 da Lei nº 14133, de 2021)

7.13. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

7.14. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

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

7.16. Os serviços serão recebidos definitivamente no prazo de 5 (cinco) dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

7.16.1. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento (art. 21, VIII, Decreto nº 11.246, de 2022).

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

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

7.16.4. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

7.16.5. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.

7.17. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

7.18. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

7.19. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

Liquidação

7.20. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022.

7.21. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, nos casos de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021

7.22. Para fins de liquidação, o setor competente deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

7.22.1. o prazo de validade;

7.22.2. a data da emissão;

7.22.3. os dados do contrato e do órgão contratante;

7.22.4. o período respectivo de execução do contrato;

7.22.5. o valor a pagar; e

7.22.6. eventual destaque do valor de retenções tributárias cabíveis.

7.23. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus à contratante;

7.24. A Nota Fiscal ou Fatura 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. 68 da Lei nº 14.133/2021.

7.25. A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas (INSTRUÇÃO NORMATIVA Nº 3, DE 26 DE ABRIL DE 2018).

7.26. Constatando-se, junto ao SICAF, a situação de irregularidade do contratado, 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 contratante.

7.27. Não havendo regularização ou sendo a defesa considerada improcedente, o contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, 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.

7.28. Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

7.29. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação junto ao SICAF.

Prazo de pagamento

7.30. O pagamento será efetuado no prazo máximo de até 10 (dez) dias úteis, contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

7.31. No caso de atraso pelo Contratante, os valores devidos ao contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice IPCA de correção monetária.

Forma de pagamento

7.32. O pagamento será realizado através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

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

7.34. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

7.35. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

7.36. O contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

8. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO

Forma de seleção e critério de julgamento da proposta

8.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo de **MENOR PREÇO GLOBAL.**

Regime de execução

8.2. O regime de execução do contrato será o de empreitada por preço global.

Exigências de habilitação

8.3. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

Habilitação jurídica

8.4. **Pessoa física:** cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

8.5. **Empresário individual**: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

8.6. **Microempreendedor Individual - MEI**: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br/empreendedor;

8.7. Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

8.8. **Sociedade empresária estrangeira**: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020.

8.9. **Sociedade simples**: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

8.10. **Filial, sucursal ou agência de sociedade simples ou empresária**: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz

8.11. **Sociedade cooperativa**: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

8.12. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

Habilitação fiscal, social e trabalhista

8.13. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

8.14. 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 administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

8.15. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

8.16. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

8.17. Prova de inscrição no cadastro de contribuintes Estadual/Distrital e/ou Municipal/Distrital relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

8.18. Prova de regularidade com a Fazenda Estadual/Distrital e/ou Municipal/Distrital do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

8.19. Caso o fornecedor seja considerado isento dos tributos Estadual/Distrital ou Municipal/Distrital relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

8.20. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

Qualificação Econômico-Financeira

8.21. Apresentação do Balanço Patrimonial acompanhado do termo de abertura e encerramento do Livro Diário e demonstração de Resultado Econômico contábil do último exercício social, já exigíveis e apresentados na forma da Lei, comprovando a boa situação da empresa, vedada a substituição por balancetes ou balanços provisórios, dispensando-se da apresentação as constituídas há menos de um ano, que não encerraram seu primeiro exercício.

8.22. As empresas obrigadas por lei a apresentar ECD – Escrituração Contábil Digital, deverão juntar o respectivo comprovante de transmissão ao SPED (Sistema Público de Escrituração Digital), bem como o Balanço Patrimonial (Instrução Normativa RFB nº 2.003, de 18 de janeiro de 2021).

8.23. Comprovação, firmada por contador da licitante, da boa situação da empresa, que será avaliada por meio dos seguintes índices financeiros a serem extraídos do balanço do último exercício social da empresa:

a) Índice de Liquidez Corrente:
ILC = Ativo Circulante ≥ 1,00 (um)
Passivo Circulante

b) Índice de Liquidez Geral:
ILG = Ativo Circulante + Realizável a Longo Prazo ≥ 1,00 (um)
Passivo Circulante + Exigível a Longo Prazo

8.24. O atendimento dos índices econômicos previstos neste termo de referência deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

8.25. Certidão Negativa de existência de processo falimentar ou de recuperações previstas na Lei Federal nº 11.101 de 09/02/2005 ou, mesmo, de concordata em nome da licitante ajuizada em data anterior ao

advento do diploma legal citado, expedida pelo distribuidor da sede da pessoa jurídica. A certidão requerida deve apresentar data inferior a 90 (noventa) dias da entrega das propostas;

8.26. A apresentação da contestação do pedido de falência, enquanto não proferida a sentença, deverá ser levada em conta pela Comissão de Licitação para efeito de qualificação econômico-financeira.

Qualificação Técnica

8.27. **Declaração da proponente atestando que todos os equipamentos ofertados são novos**, de primeiro uso e os modelos cotados não estão sofrendo processo de descontinuação, e caso ocorram serão substituídos por novos modelos de mesma especificação ou superior, sem custo adicional, bem como, que garante as atualizações corretivas e evolutivas dos programas durante todo o período contratado, sem custos;

Certificações Técnicas:

8.28. **Declaração formal de disponibilidade técnica**, assinada por seu representante legal, em papel timbrado da licitante, atestando que possui estrutura adequada e 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, incluindo atendimento a requisitos de suporte técnico e gestão de incidentes de segurança, conforme modelo constante do Anexo VI, devendo comprovar, no mínimo:

8.29. 1 (um) profissional com certificação em tecnologias de firewall e segurança de rede (ex: certificações fornecidas pelos fabricantes de NGFW como Fortinet, Palo Alto, Cisco, entre outros);

8.30. 1 (um) profissional com certificação ou qualificação técnica em sistemas de monitoramento e armazenamento de logs (ex: SIEM, Splunk, ELK Stack, FortiAnalyzer).

8.31. Apresentar catálogos, prospectos, folders, manuais e outros documentos e informações sob a marca, fabricante, modelo e outros dados pertinentes que permitam a clara e segura identificação do produto ofertado, em idioma português ou inglês, em original ou cópia, não sendo aceitos documentos impressos de qualquer natureza produzidos com a finalidade específica de possibilitar e qualificar tecnicamente a proposta da licitante. Os documentos poderão ser entregues em formato eletrônico;

8.32. Documentos obtidos pela Internet no site do fabricante do software, cujas páginas deverão ter a indicação do endereço URL em que foram obtidas;

8.33. Visando comprovar o atendimento aos requisitos técnicos, o vencedor deverá informar com base nos descritivos técnicos do firewall/Sdwan os trechos da documentação que comprovem os respectivos requisitos exigidos devem estar grifados/destacados nos documentos enviados (catálogos, folders, datasheets), de forma a facilitar sua identificação e visualização;

Declaração de Capacidade Técnica

8.34. **Atestado de vistoria** assinado pelo responsável técnico do CRCMG, conforme modelo constante do Anexo IV, ou **Declaração de ciência das informações e condições do local de execução dos**

serviços, conforme modelo constante do Anexo V, assinada por representante do licitante, assumindo todos riscos e consequências relativos às condições dos locais de execução do objeto e peculiaridades inerentes à natureza do trabalho, podendo o licitante, escolher entre as duas opções, a que melhor estiver adequada para sua participação no certame.

Qualificação Técnico-Operacional

8.35. Comprovação similar, de complexidade tecnológica e operacional equivalente ou superior à do objeto desta contratação, ou do item pertinente, por meio da apresentação de certidões ou atestados emitidos por pessoas jurídicas de direito público ou privado, ou pelo conselho profissional competente, quando for o caso.

8.36. Para fins da comprovação de que trata este subitem, as documentações deverão dizer respeito a contrato(s) executado(s) com as seguintes características mínimas:

8.36.1. Atestado(s) que comprove(m) a experiência mínima de 1 (um) ano do fornecedor na prestação dos serviços de firewall de próxima geração (NGFW) em períodos sucessivos ou não, sendo aceito o somatório de atestados de períodos diferentes.

8.36.2. Apresentar no mínimo 1 (um) contrato que comprove a experiência do fornecedor na prestação dos serviços de Zero Trust (Confiança Zero).

8.36.3. Serão admitidos, para fins de comprovação de quantitativo mínimo de serviço, a apresentação e o somatório de diferentes atestados de serviços executados de forma concomitante, pois essa situação equivale, para fins de comprovação de capacidade técnico-operacional, a uma única contratação.

8.36.4. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

8.36.5. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual do Contratante e local em que foram prestados os serviços, entre outros documentos.

8.36.6. Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

8.37. Serão aceitos atestados ou outros documentos hábeis emitidos por entidades estrangeiras quando acompanhados de tradução para o português, salvo se comprovada a inidoneidade da entidade emissora.

8.38. A apresentação, pelo fornecedor, de certidões ou atestados de desempenho anterior emitido em favor de consórcio do qual tenha feito parte será admitida, desde que atendidos os requisitos do art. 67, §§ 10 e 11, da Lei nº 14.133/2021 e regulamentos sobre o tema.

8.39. Caso admitida a participação de cooperativas, será exigida a seguinte documentação complementar:

8.40. A relação dos cooperados que atendem aos requisitos técnicos exigidos para a contratação e que executarão o contrato, com as respectivas atas de inscrição e a comprovação de que estão domiciliados

na localidade da sede da cooperativa, respeitado o disposto nos arts. 4º, inciso XI, 21, inciso I e 42, §§2º a 6º da Lei n. 5.764, de 1971;

8.41. A declaração de regularidade de situação do contribuinte individual – DRSCI, para cada um dos cooperados indicados;

8.42. A comprovação do capital social proporcional ao número de cooperados necessários à prestação do serviço;

8.43. O registro previsto na Lei n. 5.764, de 1971, art. 107;

8.44. A comprovação de integração das respectivas quotas-partes por parte dos cooperados que executarão o contrato;

8.45. Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa: a) ata de fundação; b) estatuto social com a ata da assembleia que o aprovou; c) regimento dos fundos instituídos pelos cooperados, com a ata da assembleia; d) editais de convocação das três últimas assembleias gerais extraordinárias; e) três registros de presença dos cooperados que executarão o contrato em assembleias gerais ou nas reuniões seccionais; e f) ata da sessão que os cooperados autorizaram a cooperativa a contratar o objeto da licitação; e

8.46. A última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei n. 5.764, de 1971, ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador

9. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

9.1. O custo estimado total da contratação é de R$ R$ 523.500,00 (quinhentos e vinte e três mil e quinhentos reais), conforme custos unitários apostos na tabela abaixo.

ITEM	ESPECIFICAÇÃO	CATSER	UNIDADE DE MEDIDA	QTD	VALOR MENSAL + PERCELA ÚNICA	VALOR TOTAL ESTIMADO – 60 MESES
1	1.1 Firewall da Próxima Geração (NGFW); Modelo de referência: FG-90G da Fortinet (equivalente ou superior)	609340	Dispositivo (Mês)	1	R$ 8.725,00	R$ 523.500,00
	1.2 Plataforma de Zero Trust (Confiança Zero) para o mínimo de 100 usuários;		Usuários (Mês)	100		
	1.3 Plataforma de gerenciamento, monitoramento e armazenamento de logs;		Dispositivo (Mês)	1		
	1.4 Serviços profissionais de suporte técnico em toda solução;		Suporte técnico (Mês)	1		
	1.5 Serviços profissionais de implementação da solução;		Implementação (Único)	1		
	1.6 Operação assistida;		Operação assistida (Único)	5 dias		
	1.7 Treinamento Hands On da operação do ambiente;		Usuários (Único)	2		

10. ADEQUAÇÃO ORÇAMENTÁRIA

10.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados em dotação orçamentária própria.

10.1.1. A contratação será atendida pela seguinte dotação:

a) Projeto: 5002 – Tecnologia da Informação
b) Conta Contábil: 6.3.1.3.02.01.005
c) Centro de Custo: 327 – Gerência de Tecnologia da Informação.

10.2. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Plano de Trabalho do respectivo exercício.

11. RESPONSÁVEL PELA ELABORAÇÃO

Assinado eletronicamente por:
Cláudio Márcio Araújo da Silva
CPF: [redacted]
Data: 21/03/2025 07:40:13 -03:00

GERENTE DE TECNOLOGIA DA INFORMAÇÃO

Assinado digitalmente por:
IZAIAS ANGELO GOMES
CPF: [redacted]
Certificado emitido por AC SyngularID Multipla
Data: 21/03/2025 08:17:01 -03:00

GERENTE DE CONTRATAÇÕES

Assinado digitalmente por:
SUELY MARIA MARQUES DE OLIVEIRA
CPF: [redacted]
Certificado emitido por AC SOLUTI Multipla v5
Data: 21/03/2025 09:45:03 -03:00

PRESIDENTE

MANIFESTO DE ASSINATURAS

Código de validação: RAGAG-537CD-KQECQ-9VL6F

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

- ✔ Cláudio Márcio Araújo da Silva (CPF [redacted]) em 21/03/2025 07:40 - Assinado eletronicamente

Endereço IP	Geolocalização
187.111.24.82	Lat: -19,936051 Long: -43,925504 Precisão: 4620 (metros)

Autenticação [redacted]

Login

Es3QcFvpVUwvsSnoNETB+o9+DJI3buRjEYQvs/Nr8g8=

SHA-256

- ✔ IZAIAS ANGELO GOMES (CPF 046.926.156-05) em 21/03/2025 08:17 - Assinado com certificado digital ICP-Brasil
- ✔ SUELY MARIA MARQUES DE OLIVEIRA (CPF 686.588.426-49) em 21/03/2025 09:45 - Assinado com certificado digital ICP-Brasil

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

https://assinador.crcmg.org.br/validate/RAGAG-537CD-KQECQ-9VL6F

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

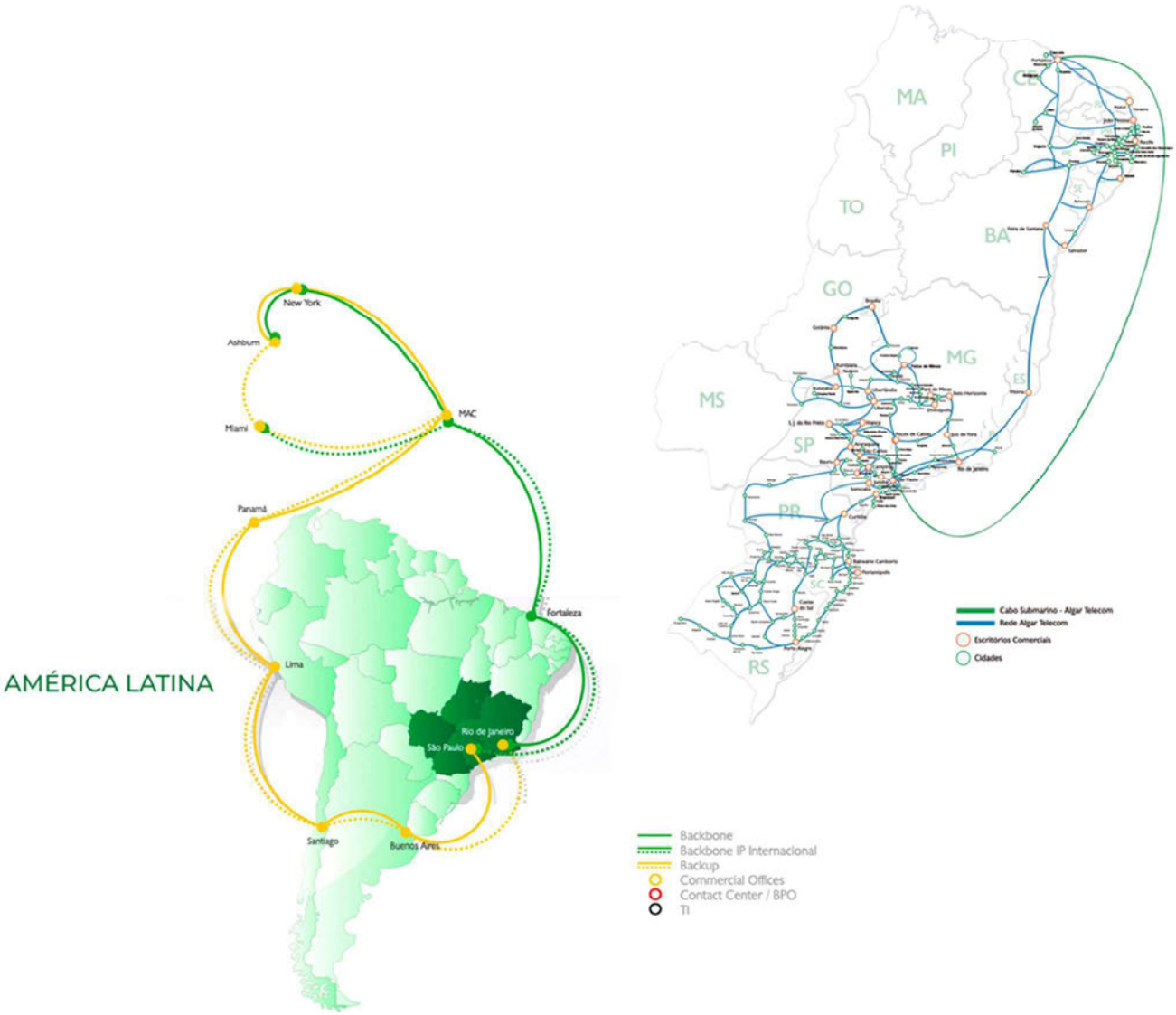
https://assinador.crcmg.org.br/validate

PROPOSTA COMERCIAL

Algar Telecom

Somos a empresa de telecomunicações e tecnologia da informação que faz parte do grupo Algar. Na Algar Telecom, trabalhamos com tecnologia para trazer soluções que conectem as pessoas e melhorem o desempenho das empresas. Acreditamos na inovação para levar produtos e serviços cada vez mais eficientes e assertivos para os nossos clientes.

Nossas soluções chegam a 372 cidades, distribuídas em 16 estados brasileiros e no Distrito Federal. Produtos e serviços de conectividade são a base para a vida contemporânea e fazem parte da inclusão digital do país.



Nossa qualidade é reconhecida

Valor Inovação 2023
Conquistamos o prêmio de 3ª empresa mais inovadora do país no setor de Telecomunicações

Melhores do ESG EXAME 2023
Algar Telecom eleita por 10 anos consecutivos como a Telecom mais sustentável do país pela Revista Exame

Great Place to Work® - Brasil 2022
Melhores empresas para trabalhar no Brasil

Prêmio Valor Inovação Brasil 2022
Terceira empresa mais inovadora no setor de Telecomunicações

100+ Inovadoras no Uso de TI 2022
Entre as empresas mais inovadoras no uso de TI do Brasil

Great Place to Work® - Minas Gerais 2022
Melhores empresas para trabalhar em Minas Gerais

SELO CERTIGOV:

Nossa empresa possui o selo CertiGov. Esta certificação demonstra nosso comprometimento com as boas práticas de vendas no mercado e atesta nossas ações de integridade nos processos, políticas e na disseminação da cultura ética.

Ao

CONSELHO REGIONAL DE CONTABILIDADE DE MINAS GERAIS

Prezados Senhores,

A empresa VOGEL SOLUÇÕES EM TELECOMUNICAÇÕES E INFORMÁTICA S/A, inscrita no CNPJ/MF sob o n° 05.872.814/0001-30, com sede à Av.: Professor Vicente Rao, nº 1262, Bairro Jardim Petrópolis, CEP: 04.636-001, São Paulo/SP, representada pela Sra. Luísa de Gois Aquino, portadora do RG [redacted] e inscrita no CPF nº [redacted] nos termos do presente Pregão e de acordo com as características descritas no Termo de Referência, apresenta a seguinte proposta conforme abaixo:

ESPECIFICAÇÃO DO OBJETO - Contratação de serviços de firewall de próxima geração (NGFW), Plataforma de Zero Trust (Confiança Zero) e Plataforma de gerenciamento, monitoramento e armazenamento de logs, incluindo demais serviços e treinamento Hands On, conforme condições e exigências estabelecidas neste instrumento, pelo período de 60 (sessenta meses).

PROPOSTA COMERCIAL E TABELA DE PREÇOS

Objeto: Contratação de serviços de firewall de próxima geração (NGFW), Plataforma de Zero Trust (Confiança Zero) e Plataforma de gerenciamento, monitoramento e armazenamento de logs, incluindo demais serviços e treinamento Hands On, pelo período de 60 (sessenta meses), conforme condições, quantidades e exigências estabelecidas no respectivo Edital e seus anexos.

ITEM	ESPECIFICAÇÃO	UNIDADE DE MEDIDA	QTD	VALOR UNITÁRIO	VALOR TOTAL POR 60 MESES
1	1.1 Firewall da Próxima Geração (NGFW);	Dispositivo (Mês)	1	R$ 2.690,00	R$ 161.400,00
	1.2 Plataforma de Zero Trust (Confiança Zero) para o mínimo de 100 usuários;	Usuários (Mês)	100	R$ 20,00	R$ 120.000,00
	1.3 Plataforma de gerenciamento, monitoramento e armazenamento de logs;	Dispositivo (Mês)	1	R$ 1.500,00	R$ 90.000,00
	1.4 Serviços profissionais de suporte técnico em toda solução;	Suporte técnico (Mês)	1	R$ 1.500,00	R$ 90.000,00
	1.5 Serviços profissionais de implementação da solução;	Implementação (Único)	1	R$ -	R$ -
	1.6 Operação assistida;	Operação assistida (Único)	5 dias	R$ -	R$ -
	1.7 Treinamento Hands On da operação do ambiente.	Usuários (Único)	2	R$ -	R$ -
	VALOR TOTAL 60 (SESSENTA) MESES TODOS OS SERVIÇOS				R$ 461.400,00

Validade da Proposta: 120 (cento e vinte) dias.

Para os serviços com unidade de medida "mês" deverão ter seus valores unitários multiplicados pelo período de 60 (sessenta) meses.

Para os serviços com unidade de medida "único" deverão ter seus valores unitários replicados na coluna "valor total por 60 meses", sem qualquer multiplicação.

Condições de pagamento conforme disposições previstas no respectivo Edital e seus anexos.

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 004/2025, inclusive quanto ao cumprimento na íntegra do respectivo Termo de Referência - Anexo I.

Declaramos que nos preços propostos estão computados todos os custos básicos que incidam ou venham a incidir, direta ou indiretamente, sobre o objeto do Pregão, inclusive tributos, contribuições incidentes, impostos, taxas, encargos sociais, fretes até o destino e quaisquer outros ônus que porventura possam recair sobre o objeto do presente pregão.

Declaramos que concordamos integralmente com as condições estipuladas na presente licitação, que se vencedor deste certame, nos submeteremos ao cumprimento de seus termos.

CONSULTOR DESIGNADO PARA ATENDIMENTO AO CLIENTE

Gustavo Rodrigues Coimbra
Consultor de Vendas Diretas
Telefone comercial - (31) 986044338
Email - gustavo.coimbra@algartelecom.com.br

DADOS COMPLETOS DA EMPRESA

Razão Social: VOGEL SOLUÇÕES EM TELECOMUNICAÇÕES E INFORMÁTICA S/A
CNPJ: 05.872.814/0001-30
Inscrição Estadual: 001.030.140.0075
Inscrição Municipal: 183.0800
Endereço: Av.: Professor Vicente Rao, nº 1262, Bairro Jardim Petrópolis,
CEP: 04.636-001, São Paulo/SP

DADOS DOS REPRESENTANTES LEGAIS DA EMPRESA PARA ASSINATURA DO CONTRATO:

1 - Nome: Jeankarlo Rodrigues da Cunha
Cargo: Gerente de Negócios Governo
CPF: [redacted]
RG: [redacted]

2 - Nome: Luísa de Gois Aquino
Cargo: Analista Licitação
CPF: [redacted]
RG: [redacted]

DADOS BANCÁRIO

Banco: Itaú
Nº do Banco: [redacted]
Agência: [redacted]
Conta corrente: [redacted]

DADOS PARA PAGAMENTO

O procedimento de apresentação de fatura (nota fiscal com código de barras) ou via SIAFI, nos casos de órgãos vinculados à Administração Pública Federal, como é o caso da ANATEL, tendo em vista que o sistema de boleto permite a identificação célere do pagamento e a correta retenção dos impostos

diretamente, sendo, pois, menores os riscos de problemas relacionados às emissões de faturas. Isto posto, entendemos que os pagamentos poderão ser via boleto com código de barras.

Caso opte por pagamentos via depósitos, solicitamos o envio das informações abaixo para o e-mail cobranca.governo@algartelecom.com.br para conclusão das baixas.

A empresa está participando desse processo com os dados da matriz da companhia que tem sede no Estado de São Paulo, contudo cabe esclarecer que, no ato do faturamento dos seus serviços a companhia está obrigada a observar as disposições contidas na legislação tributária-fiscal, conforme a natureza jurídica tributária-fiscal do serviço que será instalado e prestado. Serviços de telecomunicações são regidos pela LC nº 87/96 e o faturamento deverá ocorrer conforme disposto na alínea "d" do artigo 11 (local das prestações dos serviços). Em sendo serviços de tecnologia o faturamento seguirá as regras do art. 3º da LC nº 116/2003 e o faturamento deverá ocorrer pelo estabelecimento que concentra os recursos necessários para a prestação dos serviços. Importante frisar que filiais e matriz são a mesma pessoa jurídica, sendo a filial um dos domicílios da pessoa jurídica, conforme § 1º do art. 75 do CC. Em termos fiscais a RFB exige que cada domicílio da empresa possua cadastro, contudo o próprio cadastro deriva da matriz da pessoa jurídica, logo todas as filiais terão a mesma base do cadastro de pessoa jurídica.

DADOS DO PAGAMENTO

- ✓ Nome do órgão
- ✓ CNPJ do órgão
- ✓ N° do Contrato
- ✓ Banco e Agência
- ✓ Data do depósito
- ✓ Valor total do depósito
- ✓ Vencimento da conta
- ✓ Favorecido
- ✓ Número da fatura
- ✓ Valor da fatura
  * Caso haja glosa informar motivo e valor

- ➢ **Atenção:** Caso não seja enviado as informações acima dentro do prazo de 5 (cinco) dias úteis, será dado as baixas a partir das faturas mais antigas pendentes.

INFORMAÇÕES COMPLEMENTARES

SAC Atendimento Governo/empresas: 0800 940 0612 (24 x 7).

Portal de autoatendimento, onde você consegue ter acesso (Faturas / Contestação / Chamados / Desbloqueio em Confiança / Produtos Ativos / Etc...)

Segue abaixo o link.

PORTAL DE ATENDIMENTO (Clique com botão direito e selecione Abrir Hiperlink)

Enviar o contrato para assinatura por parte desta empresa, para o seguinte destinatário:

ALGAR TELECOM S/A
A/C: Gestão de Contratos Governo – Coordenação de Vendas Governo
Rua José Alves Garcia, nº 415, Bairro: Brasil
CEP: 38.400-668, Uberlândia/MG

Contatos:
Nome: Karlla Christina Ferreira
Telefone: (34) 3256-2820 (34)99643 0013
E-mail: contratosgoverno@algartelecom.com.br

Uberlândia, 28 de abri de 2025.

LUISA DE GOIS AQUINO [redacted] Assinado de forma digital por LUISA DE GOIS AQUINO:[redacted]

Luísa de Gois Aquino
Consultora de Vendas Governo
CPF [redacted]
RG [redacted]

MANIFESTO DE ASSINATURAS

Código de validação: PV4LG-C4U59-GAMSV-4W4YV

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

- KLEVER JOAO DOS SANTOS (CPF [redacted]) em 28/05/2025 08:38 - Assinado com certificado digital ICP-Brasil
- JEANKARLO RODRIGUES DA CUNHA (CPF [redacted]) em 28/05/2025 15:09 - Assinado com certificado digital ICP-Brasil
- WATSON BONIFACIO DA SILVA (CPF [redacted]) em 28/05/2025 15:10 - Assinado com certificado digital ICP-Brasil
- CLAUDIO MARCIO ARAUJO DA SILVA (CPF [redacted]) em 28/05/2025 15:12 - Assinado com certificado digital ICP-Brasil
- WILLIAN FERNANDO DE FREITAS (CPF [redacted]) em 28/05/2025 15:34 - Assinado com certificado digital ICP-Brasil
- SUELY MARIA MARQUES DE OLIVEIRA (CPF [redacted]) em 28/05/2025 15:43 - Assinado com certificado digital ICP-Brasil

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

https://assinador.crcmg.org.br/validate/PV4LG-C4U59-GAMSV-4W4YV

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

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