



CONSELHO REGIONAL DE MEDICINA DO ESTADO DE MINAS GERAIS

MINUTA DE EDITAL

Belo Horizonte, 21 de agosto de 2026

CAPA

Pregão:13/2026

ComprasGov nº. 389172-25/2026

Contratante: 389172

Orgão: CONSELHO REGIONAL DE MEDICINA DO ESTADO DE MINAS GERAIS

CNPJ: 22.256.879/0001-70

Setor: Compras e Licitações

Endereço: Rua dos Timbiras, número 1200, Bairro Boa Viagem, Belo Horizonte/MG, CEP : 30140060

Objeto: Aquisição de Solução Integrada de Segurança da Informação, em lote único, contemplando o fornecimento, implantação, configuração, suporte técnico, garantia, licenciamento, atualizações e transferência de conhecimento, pelo período de 60 (sessenta) meses, incluindo firewalls de próxima geração, equipamento de gerenciamento centralizado, switches, access points, solução de detecção e resposta de endpoint — XDR, serviço de instalação e configuração e treinamento oficial do fabricante.

Valor: R\$ 2.586.813,19

Sigiloso: Não

Processo: 26.13.000003312-0

SRP: Não

Critério de Julgamento: MENOR PREÇO

Modalidade: Aberto

Preferência ME EPP: Não

Margem de Preferência: Não

Data da Sessão: 15/09/2026

Hora Inicial: 14:00

MODELO DE EDITAL

PREGÃO ELETRÔNICO
CONSELHO REGIONAL DE MEDICINA DO ESTADO DE MINAS GERAIS

PREGÃO ELETRÔNICO Nº 13/2026

ComprasGov Nº. 389172-25/2026

Processo Administrativo nº 26.13.000003312-0

Torna-se público, para conhecimento dos interessados, que o(a) CONSELHO REGIONAL DE MEDICINA DO ESTADO DE MINAS GERAIS, CNPJ 22.256.879/0001-70, por meio do(a) Compras e Licitações, sediado(a) DOS TIMBIRAS, 1200, bairro Boa Viagem, na cidade de BELO HORIZONTE/MG, CEP 30140060, realizará licitação, na modalidade Pregão Eletrônico, na forma Eletrônica, com critério de julgamento Menor Preço, [Lei nº 14.133, de 1º de abril de 2021](#), e demais legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital.

Data da Sessão Pública: **15/09/2026**

Hora Inicial : 14:00



Documento assinado eletronicamente por **Lívia Pinheiro de Azevedo, Coordenador(a) do Setor de Compras e Licitação do CRM-MG**, em 21/08/2026, às 15:15, com fundamento no art. 5º da [RESOLUÇÃO CFM nº2.308/2022, de 28 de março de 2022](#).



A autenticidade do documento pode ser conferida no site https://sei.cfm.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **4758927** e o código CRC **A8E701D8**.



Rua dos Timbiras, 1200 - Bairro Boa Viagem |
CEP 30140-064 | Belo Horizonte/MG -
<https://www.crmmg.org.br/>



Referência: Processo SEI nº 26.13.000003312-0 | data de inclusão: 21/08/2026



CONSELHO REGIONAL DE MEDICINA DO ESTADO DE MINAS GERAIS

MINUTA DE EDITAL

Belo Horizonte, 13 de agosto de 2026

CAPA

Pregão:13/2026

ComprasGov nº. XX/2026

Contratante: 389172

Orgão: CONSELHO REGIONAL DE MEDICINA DO ESTADO DE MINAS GERAIS

CNPJ: 22.256.879/0001-70

Setor: Compras e Licitações

Endereço: Rua dos Timbiras, número 1200, Bairro Boa Viagem, Belo Horizonte/MG, CEP : 30140060

Objeto: Aquisição de Solução Integrada de Segurança da Informação, em lote único, contemplando o fornecimento, implantação, configuração, suporte técnico, garantia, licenciamento, atualizações e transferência de conhecimento, pelo período de 60 (sessenta) meses, incluindo firewalls de próxima geração, equipamento de gerenciamento centralizado, switches, access points, solução de detecção e resposta de endpoint — XDR, serviço de instalação e configuração e treinamento oficial do fabricante.

Valor: R\$ 2.586.813,19

Sigiloso: Não

Processo: 26.13.000003312-0

SRP: Não

Critério de Julgamento: MENOR PREÇO

Modalidade: Aberto

Preferência ME EPP: Não

Margem de Preferência: Não

Data da Sessão: XX/XX/2026

Hora Inicial: 14:00

MODELO DE EDITAL

PREGÃO ELETRÔNICO
CONSELHO REGIONAL DE MEDICINA DO ESTADO DE MINAS GERAIS

PREGÃO ELETRÔNICO Nº 13/2026

ComprasGov Nº. XX/2026

Processo Administrativo nº 26.13.000003312-0

Torna-se público, para conhecimento dos interessados, que o(a) CONSELHO REGIONAL DE MEDICINA DO ESTADO DE MINAS GERAIS, CNPJ 22.256.879/0001-70, por meio do(a) Compras e Licitações, sediado(a) DOS TIMBIRAS, 1200, bairro Boa Viagem, na cidade de BELO HORIZONTE/MG, CEP 30140060, realizará licitação, na modalidade Pregão Eletrônico, na forma Eletrônica, com critério de julgamento Menor Preço, [Lei nº 14.133, de 1º de abril de 2021](#), e demais legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital.

Data da Sessão Pública: **XX/XX/2026**

Hora Inicial : 14:00

1. DO OBJETO

1.1. O objeto da presente licitação é Aquisição de Solução Integrada de Segurança da Informação, em lote único, contemplando o fornecimento, implantação, configuração, suporte técnico, garantia, licenciamento, atualizações e transferência de conhecimento, pelo período de 60 (sessenta) meses, incluindo firewalls de próxima geração, equipamento de gerenciamento centralizado, switches, access points, solução de detecção e resposta de endpoint — XDR, serviço de instalação e configuração e treinamento oficial do fabricante, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2. A licitação será realizada em grupo único, formado por 11 (onze) itens, conforme tabela constante no Termo de Referência/Projeto Básico, devendo o licitante oferecer proposta para todos os itens que o compõem.

2. DA PARTICIPAÇÃO NA LICITAÇÃO

2.1. Poderão participar deste certame os interessados cujo ramo de atividade seja compatível com o objeto da licitação e que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras).

2.2. Os interessados deverão atender às condições exigidas no cadastramento no Sicaf até o terceiro dia útil anterior à data prevista para recebimento das propostas.

2.3. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluindo a responsabilidade do provedor do

sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

2.4. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais nos Sistemas relacionados no item anterior e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

2.5. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.

2.6. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no [art. 16 da Lei nº 14.133, de 2021](#), para o agricultor familiar, o produtor rural pessoa física e para o microempreendedor individual - MEI, nos limites previstos da [Lei Complementar nº 123 de 2006](#).

2.7. Será concedido tratamento favorecido para bens e serviços produzidos com tecnologia produzida no país e bens produzidos de acordo com processo produtivo básico, na forma do art. 3º da [Leis nº 8.248, de 23 de outubro de 1991](#) e art. 8º do Decreto nº 7.174, de 2010.

2.8. Não poderão disputar esta licitação:

2.8.1. aquele que não atenda às condições deste Edital e seu(s) anexo(s);

2.8.2. sociedade que desempenhe atividade incompatível com o objeto da licitação;

2.8.3. empresas estrangeiras que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;

2.8.4. autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a licitação versar sobre serviços ou fornecimento de bens a ele relacionados;

2.8.5. empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a licitação versar sobre serviços ou fornecimento de bens a ela necessários;

2.8.6. pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

2.8.7. aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe 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;

2.8.8. empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1986, concorrendo entre si;

2.8.9. pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista;

2.8.10. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;

2.9. Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público do órgão ou entidade contratante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme [§ 1º do art. 9º da Lei nº 14.133, de](#)

[2021.](#)

2.10. O impedimento de que trata o item 2.8.6 será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

2.11. A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem os itens 2.8.4 e 2.8.5 poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.

2.12. Equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico.

2.13. O disposto nos itens 2.8.4 e 2.8.5 não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.

2.14. Em licitações e contratações realizadas no âmbito de projetos e programas parcialmente financiados por agência oficial de cooperação estrangeira ou por organismo financeiro internacional com recursos do financiamento ou da contrapartida nacional, não poderá participar pessoa física ou jurídica que integre o rol de pessoas sancionadas por essas entidades ou que seja declarada inidônea nos termos da [Lei nº 14.133, de 2021](#).

2.15. A vedação de que trata o item 2.9 estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

3. ORÇAMENTO ESTIMADO SIGILOSO

3.1. O orçamento estimado da presente contratação não será de caráter sigiloso.

4. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

4.1. Na presente licitação, a fase de habilitação sucederá as fases de apresentação de propostas e lances e de julgamento.

4.2. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com o preço, conforme o critério de julgamento adotado neste Edital, até a data e o horário estabelecidos para abertura da sessão pública.

4.3. No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema, que:

4.3.1. está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

4.3.2. não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos

termos do [artigo 7º, XXXIII, da Constituição](#);

4.3.3. não possui empregados executando trabalho degradante ou forçado, observando o disposto nos [incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal](#);

4.3.4. cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

4.4. O licitante organizado em cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no [artigo 16 da Lei nº 14.133, de 2021](#).

4.5. Não poderá se beneficiar do tratamento jurídico diferenciado estabelecido nos arts. 42 a 49 da Lei Complementar nº 123, de 2006, a pessoa jurídica:

4.5.1. de cujo capital participe outra pessoa jurídica;

4.5.2. que seja filial, sucursal, agência ou representação, no País, de pessoa jurídica com sede no exterior;

4.5.3. de cujo capital participe pessoa física que seja inscrita como empresário ou seja sócia de outra empresa que receba tratamento jurídico diferenciado nos termos da Lei Complementar nº 123, de 2006, desde que a receita bruta global ultrapasse o limite de que trata o inciso II do art. 3º da referida lei;

4.5.4. cujo titular ou sócio participe com mais de 10% (dez por cento) do capital de outra empresa não beneficiada pela Lei Complementar nº 123, de 2006, desde que a receita bruta global ultrapasse o limite de que trata o inciso II do art. 3º da referida lei;

4.5.5. cujo sócio ou titular seja administrador ou equiparado de outra pessoa jurídica com fins lucrativos, desde que a receita bruta global ultrapasse o limite de que trata o inciso II do art. 3º da referida lei;

4.5.6. constituída sob a forma de cooperativas, salvo as de consumo;

4.5.7. que participe do capital de outra pessoa jurídica;

4.5.8. que exerça atividade de banco comercial, de investimentos e de desenvolvimento, de caixa econômica, de sociedade de crédito, financiamento e investimento ou de crédito imobiliário, de corretora ou de distribuidora de títulos, valores mobiliários e câmbio, de empresa de arrendamento mercantil, de seguros privados e de capitalização ou de previdência complementar;

4.5.9. resultante ou remanescente de cisão ou qualquer outra forma de desmembramento de pessoa jurídica que tenha ocorrido em um dos 5 (cinco) anos-calendário anteriores;

4.5.10. constituída sob a forma de sociedade por ações.

4.5.11. cujos titulares ou sócios guardem, cumulativamente, com o contratante do serviço, relação de pessoalidade, subordinação e habitualidade.

4.6. O licitante deverá declarar em campo próprio do sistema que desenvolve programa de integridade, nos termos do Decreto nº 12.304, de 2024, e da [Portaria Normativa SE/CGU nº 226, de 9 de setembro de 2025](#), para fazer jus ao benefício do critério de desempate previsto no art. 60, caput, inciso IV, da lei n. 14.133, de 2021.

4.7. A falsidade da declaração de que trata os itens 4

4.8. Os licitantes poderão retirar ou substituir a proposta ou, na hipótese de a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, os documentos de habilitação anteriormente inseridos no sistema, até a abertura da sessão pública.

4.9. Não haverá ordem de classificação na etapa de apresentação da proposta e dos

documentos de habilitação pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.

4.10. Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para apresentação de propostas, após a fase de envio de lances.

4.11. Desde que disponibilizada a funcionalidade no sistema, o licitante poderá parametrizar o seu valor final mínimo ou o seu percentual de desconto máximo quando do cadastramento da proposta e obedecerá às seguintes regras:

4.11.1. a aplicação do intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta; e

4.11.2. os lances serão de envio automático pelo sistema, respeitado o valor final mínimo, caso estabelecido, e o intervalo de que trata o subitem acima.

4.12. O valor final mínimo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado valor superior a lance já registrado pelo fornecedor no sistema.

4.13. O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do item 4.11 possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

4.14. Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pela Administração ou de sua desconexão.

4.15. O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

5. DO PREENCHIMENTO DA PROPOSTA

5.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

grupo

5.1.1. Valor unitário e total expresso em Reais (R\$).

5.2. Todas as especificações do objeto contidas na proposta vinculam o licitante.

5.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

5.4. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

5.5. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.

5.5.1. No regime de incidência não-cumulativa de PIS e COFINS, a cotação adequada será a que

corresponde à média das alíquotas efetivamente recolhidas pela empresa, comprovada, a qualquer tempo, por documentos de Escrituração Fiscal Digital da Contribuição (EFD-Contribuições) para o PIS/PASEP e COFINS dos últimos 12 (doze) meses anteriores à apresentação da proposta, ou por outro meio hábil.

5.6. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.

5.7. Na presente licitação, a Microempresa e a Empresa de Pequeno Porte poderão se beneficiar do regime de tributação pelo Simples Nacional.

5.8. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência/Projeto Básico, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

5.9. O prazo de validade da proposta não será inferior a 60 (sessenta) dias, a contar da data de sua apresentação.

5.10. Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais, quando participarem de licitações públicas;

5.11. Os licitantes devem respeitar os preços máximos previstos no Termo de Referência/Projeto Básico;

5.12. O descumprimento das regras supramencionadas pode ensejar a responsabilização pelo Tribunal de Contas da União e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do [art. 71, inciso IX, da Constituição](#); ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

6. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

6.1. A abertura da presente licitação dar-se-á automaticamente em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

6.2. Os licitantes poderão retirar ou substituir a proposta ou os documentos de habilitação, quando for o caso, anteriormente inseridos no sistema, até a abertura da sessão pública.

6.3. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

6.4. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

6.5. O lance deverá ser ofertado pelo valor unitário do item.

6.6. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

6.7. O licitante somente poderá oferecer lance de valor inferior ao último por ele ofertado e registrado pelo sistema.

6.8. O intervalo mínimo de diferença de valor entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de R\$10,00 (dez reais).

6.9. O licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de quinze segundos após o registro no sistema, na hipótese de lance inconsistente ou inexecutável.

6.10. O procedimento seguirá de acordo com o modo de disputa aberto.

6.11. No modo de disputa “aberto”, os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

6.11.1. A etapa de lances da sessão pública terá duração de dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.

6.11.2. A prorrogação automática da etapa de lances, de que trata o subitem anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

6.11.3. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação .

6.11.4. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o , auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

6.11.5. Após o reinício previsto no item supra, os licitantes serão convocados para apresentar lances intermediários.

6.12. Após o término dos prazos estabelecidos nos subitens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

6.13. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

6.14. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

6.15. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão Eletrônico, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

6.16. Quando a desconexão do sistema eletrônico para o Pregoeiro persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.

6.17. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

6.18. Será assegurado o direito de preferência previsto no artigo 3º da [Leis nº 8.248, de 23 de outubro de 1991](#), conforme procedimento estabelecido nos artigos 5º e 8º do Decreto nº 7.174, de 2010, nos seguintes termos:

6.18.1. Após a aplicação das regras de preferência para microempresas e empresas de pequeno porte, caberá a aplicação das regras de preferência, sucessivamente, para:

6.18.1.1. bens e serviços com tecnologia desenvolvida no País e produzidos de acordo com o Processo Produtivo Básico (PPB), na forma definida pelo Poder Executivo Federal;

6.18.1.2. bens e serviços com tecnologia desenvolvida no País; e

6.18.1.3. bens e serviços produzidos de acordo com o PPB, na forma definida pelo Poder Executivo Federal, nos termos do art. 5º e 8º do Decreto 7.174, de 2010 e art. 3º da [Leis nº 8.248, de 23 de outubro de 1991](#).

6.18.2. Os licitantes classificados que estejam enquadrados no item 6.18.1.1, na ordem de classificação, serão convocados para que possam oferecer nova proposta ou novo lance para igualar ou superar a melhor proposta válida, caso em que será declarado vencedor do certame.

6.18.3. Caso a preferência não seja exercida na forma do item 6.18.1.1, por qualquer motivo, serão convocadas as empresas classificadas que estejam enquadradas no item 6.18.1.2, na ordem de classificação, para a comprovação e o exercício do direito de preferência, aplicando-se a mesma regra para o item 6.18.1.3 caso esse direito não seja exercido.

6.18.4. As licitantes qualificadas como microempresas ou empresas de pequeno porte que fizerem jus ao direito de preferência previsto no Decreto nº 7.174, de 2010, terão prioridade no exercício desse benefício em relação às médias e às grandes empresas na mesma situação.

6.19. Só poderá haver empate entre propostas iguais (não seguidas de lances).

6.20. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no [art. 60 da Lei nº 14.133, de 2021](#), nesta ordem:

6.20.5. disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;

6.20.6. avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos nesta Lei;

6.20.7. desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, nos termos do [Decreto nº 11.430, de 2023](#), e da [Instrução Normativa SEGES/MGI nº 382, de 17 de setembro de 2025](#);

6.20.8. desenvolvimento pelo licitante de programa de integridade, conforme Decreto nº 12.304, de 2024, e [Portaria Normativa SE/CGU nº 226, de 9 de setembro de 2025](#).

6.21. Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:

6.21.1. empresas estabelecidas no território do Estado ou do Distrito Federal do órgão ou entidade da Administração Pública estadual ou distrital licitante ou, no caso de licitação realizada por órgão ou entidade de Município, no território do Estado em que este se localize;

6.21.2. empresas brasileiras;

6.21.3. empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

6.21.4. empresas que comprovem a prática de mitigação, nos termos da [Lei nº 12.187, de 29 de dezembro de 2009](#).

6.22. Esgotados todos os demais critérios de desempate previstos em lei, a escolha do licitante vencedor ocorrerá por sorteio, em ato público, para o qual todos os licitantes serão convocados, vedado qualquer outro processo.

6.23. Encerrada a etapa de envio de lances da sessão pública, na hipótese da proposta do primeiro colocado permanecer acima do preço máximo definido para a contratação, o Pregoeiro poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

6.23.1. A negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido pela Administração.

6.23.2. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

6.23.3. O resultado da negociação será divulgado a todos os licitantes e anexado aos autos do processo licitatório.

6.23.4. O Pregoeiro solicitará ao licitante mais bem classificado que, no prazo de 2 (duas) horas, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

6.23.5. É facultado ao Pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

6.24. Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

7. DA FASE DE JULGAMENTO

7.1. Encerrada a etapa de negociação, o Pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133, de 2021, legislação correlata e no item 2.8 do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

7.1.1. SICAF;

7.1.2. Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS;

7.1.3. Cadastro Nacional de Empresas Punidas – CNEP e

7.1.4. Lista de licitantes inidôneos, mantida pelo Tribunal de Contas da União.

7.2. A consulta aos cadastros será realizada no nome e no CNPJ da empresa licitante.

7.2.1. A consulta no CEIS quanto às sanções previstas na [Lei nº 8.429, de 1992](#), também ocorrerá no nome e no CPF do sócio majoritário da empresa licitante, se houver, por força do art. 12 da citada lei.

7.3. Para a consulta de licitantes pessoa jurídica poderá haver a substituição das consultas ao CEIS, CNEP e Lista de licitantes inidôneos pela Consulta Consolidada de Pessoa Jurídica do TCU.

7.4. Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o Pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

7.4.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.

7.4.2. O licitante será convocado para manifestação previamente a uma eventual desclassificação.

7.4.3. Constatada a existência de sanção, o licitante será reputado inabilitado, por falta de condição de participação.

7.5. Verificadas as condições de participação e de utilização do tratamento favorecido, o Pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no [artigo 29 a 35 da IN SEGES nº 73, de 30 de setembro](#)

[de 2022.](#)

7.6. Será desclassificada a proposta vencedora que:

7.6.1. conter vícios insanáveis;

7.6.2. não obedecer às especificações técnicas contidas no Termo de Referência/Projeto Básico;

7.6.3. apresentar preços inexequíveis ou permanecer acima do preço máximo definido para a contratação;

7.6.4. não tiver sua exequibilidade demonstrada, quando exigido pela Administração;

7.6.5. não cumpra os critérios de aceitabilidade de preços definidos no Termo de Referência.

7.6.6. apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.

7.7. No caso de bens e serviços em geral, é indício de inexequibilidade das propostas valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração.

7.8. A inexequibilidade, na hipótese de que trata o item anterior, só será considerada após diligência do Pregoeiro, que comprove:

7.8.1. que o custo do licitante ultrapassa o valor da proposta; e

7.8.2. inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

7.9. Em contratação de obras e serviços de engenharia, além das disposições acima, a análise de exequibilidade e sobrepreço considerará o seguinte:

7.9.1. Nos regimes de execução por tarefa, empreitada por preço global ou empreitada integral, contratação semi-integrada ou contratação integrada, a caracterização do sobrepreço se dará pela superação do valor global estimado;

7.9.2. No regime de empreitada por preço unitário, a caracterização do sobrepreço se dará pela superação do valor global estimado.

7.9.3. No caso de obras e serviços de engenharia, serão consideradas inexequíveis as propostas cujos valores forem inferiores a 75% (setenta e cinco por cento) do valor orçado pela Administração, independentemente do regime de execução.

7.10. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que a empresa comprove a exequibilidade da proposta.

7.11. Caso o custo global estimado do objeto licitado tenha sido decomposto em seus respectivos custos unitários por meio de Planilha de Custos e Formação de Preços elaborada pela Administração, o licitante classificado em primeiro lugar será convocado para apresentar Planilha por ele elaborada, com os respectivos valores adequados ao valor final da sua proposta, sob pena de não aceitação da proposta.

7.11.1. Em se tratando de serviços de engenharia, o licitante vencedor será convocado a apresentar à Administração, por meio eletrônico, as planilhas com indicação dos quantitativos e dos custos unitários, seguindo o modelo elaborado pela Administração, bem como com detalhamento das Bonificações e Despesas Indiretas (BDI) e dos Encargos Sociais (ES), com os respectivos valores adequados ao valor final da proposta vencedora, admitida a utilização dos preços unitários, no caso de empreitada por preço global, empreitada integral, contratação semiintegrada e contratação integrada, exclusivamente para eventuais adequações indispensáveis no cronograma físico-financeiro e para balizar excepcional aditamento posterior do contrato.

7.11.2. Caso a produtividade seja diferente daquela utilizada pela Administração como

referência, ou não estiver contida na faixa referencial de produtividade, mas admitida pelo ato convocatório, o licitante deverá apresentar a respectiva comprovação de exequibilidade;

7.11.3. Os licitantes poderão apresentar produtividades diferenciadas daquela estabelecida pela Administração como referência, desde que não alterem o objeto da contratação, não contrariem dispositivos legais vigentes e, caso não estejam contidas nas faixas referenciais de produtividade, comprovem a exequibilidade da proposta.

7.11.4. Para efeito do subitem anterior, admite-se a adequação técnica da metodologia empregada pela contratada, visando assegurar a execução do objeto, desde que mantidas as condições para a justa remuneração do serviço.

7.12. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo fornecedor, no prazo indicado pelo Pregoeiro, desde que não haja majoração do preço e que se comprove que este é o bastante para arcar com todos os custos da contratação;

7.12.1. O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas;

7.12.2. Considera-se erro no preenchimento da planilha passível de correção a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime.

7.13. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante do serviço ou da área especializada no objeto.

7.14. Caso o Termo de Referência exija a apresentação de carta de solidariedade emitida pelo fabricante, que assegure a execução do contrato, no caso de licitante revendedor ou distribuidor, o licitante classificado em primeiro lugar deverá apresentá-la, sob pena de não aceitação da proposta.

7.15. Caso o Termo de Referência/Projeto Básico exija a apresentação de amostra, o licitante classificado em primeiro lugar deverá apresentá-la, conforme disciplinado no Termo de Referência, sob pena de não aceitação da proposta.

7.16. Por meio de mensagem no sistema, será divulgado o local e horário de realização do procedimento para a avaliação das amostras, cuja presença será facultada a todos os interessados, incluindo os demais licitantes.

7.17. Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

7.18. No caso de não haver entrega da amostra ou ocorrer atraso na entrega, sem justificativa aceita pelo Pregoeiro, ou havendo entrega de amostra fora das especificações previstas neste Edital, a proposta do licitante será recusada.

7.19. Se a(s) amostra(s) apresentada(s) pelo primeiro classificado não for(em) aceita(s), o Pregoeiro analisará a aceitabilidade da proposta ou lance ofertado pelo segundo classificado. Seguir-se-á com a verificação da(s) amostra(s) e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes no Termo de Referência.

8. DA FASE DE HABILITAÇÃO

8.1. Os documentos previstos no Termo de Referência, necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, serão exigidos para fins de habilitação, nos termos dos [arts. 62 a 70 da Lei nº 14.133, de 2021](#).

8.1.1. A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira, poderá ser substituída pelo registro cadastral no SICAF.

8.2. Quando permitida a participação de empresas estrangeiras que não funcionem no País, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados em tradução livre.

8.3. Na hipótese de o licitante vencedor ser empresa estrangeira que não funcione no País, para fins de assinatura do contrato ou da ata de registro de preços, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e apostilados nos termos do disposto no [Decreto nº 8.660, de 29 de janeiro de 2016](#), ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

8.4. Quando permitida a participação de consórcio de empresas, a habilitação técnica, quando exigida, será feita por meio do somatório dos quantitativos de cada consorciado e, para efeito de habilitação econômico-financeira, quando exigida, será observado o somatório dos valores de cada consorciado.

8.5. Os documentos exigidos para fins de habilitação poderão ser apresentados em original ou por cópia.

8.6. Os documentos exigidos para fins de habilitação poderão ser substituídos por registro cadastral emitido por órgão ou entidade pública, desde que o registro tenha sido feito em obediência ao disposto na Lei nº 14.133, de 2021.

8.7. Será verificado se o licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei.

8.8. Será verificado se o licitante apresentou no sistema, sob pena de inabilitação, a declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

8.9. O licitante deverá apresentar, sob pena de desclassificação, declaração de que sua proposta econômica compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

8.10. A habilitação será verificada por meio do Sicaf, nos documentos por ele abrangidos.

8.10.1. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir.

8.11. É de responsabilidade do licitante conferir a exatidão dos seus dados cadastrais no Sicaf e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

8.11.1. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.

8.12. A verificação pelo Pregoeiro, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

8.12.1. Os documentos exigidos para habilitação que não estejam contemplados no Sicaf serão enviados por meio do sistema, em formato digital, no prazo de 2 (duas) horas, prorrogável por igual período, contado da solicitação do Pregoeiro.

8.13. A verificação no Sicaf ou a exigência dos documentos nele não contidos somente será

feita em relação ao licitante vencedor.

8.13.1. Os documentos relativos à regularidade fiscal que constem do Termo de Referência somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante mais bem classificado.

8.13.2. Respeitada a exceção do subitem anterior, relativa à regularidade fiscal, quando a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, a verificação ou exigência do presente subitem ocorrerá em relação a todos os licitantes.

8.14. Encerrado o prazo para envio da documentação de que trata o item 8.12.1, poderá ser admitida, mediante decisão fundamentada do Pregoeiro, a apresentação de novos documentos de habilitação ou a complementação de informações acerca dos documentos já apresentados pelos licitantes, em até 2 (duas) horas , para:

8.14.1. a aferição das condições de habilitação do licitante, desde que decorrentes de fatos existentes à época da abertura do certame;

8.14.2. atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas;

8.14.3. suprimento da ausência de documento de cunho declaratório emitido unilateralmente pelo licitante;

8.14.4. suprimento da ausência de certidão e/ou documento de cunho declaratório expedido por órgão ou entidade cujos atos gozem de presunção de veracidade e fé pública.

8.15. Findo o prazo assinalado sem o envio da nova documentação, restará preclusa essa oportunidade conferida ao licitante, implicando sua inabilitação.

8.16. Na análise dos documentos de habilitação, a comissão de contratação poderá sanar erros ou falhas, que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

8.17. Na hipótese de o licitante não atender às exigências para habilitação, o Pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital, observado o prazo disposto no subitem 8.12.1

8.18. Somente serão disponibilizados para acesso público os documentos de habilitação do licitante cuja proposta atenda ao edital de licitação, após concluídos os procedimentos de que trata o subitem anterior.

9. DO TERMO DE CONTRATO

9.1. Após a homologação e adjudicação, caso se conclua pela contratação, será firmado termo de contrato, no prazo e condições estabelecidos neste Edital.

9.2. O adjudicatário terá o prazo de 5 (cinco) dias úteis, contados a partir da data de sua convocação, para assinar o termo de contrato, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas neste Edital.

9.3. Quando for exigida a prestação de garantia contratual e o adjudicatário optar pela modalidade seguro-garantia, ser-lhe-á assegurado o prazo mínimo de 1 (um) mês, contado da data da homologação da licitação e anterior à assinatura do contrato, para a apresentação da respectiva apólice, nos termos do art. 96, § 3º, da Lei nº 14.133/2021.

9.4. Na hipótese do item 9.3:

9.4.1. A convocação para a assinatura do contrato observará o transcurso do prazo de que trata o item 9.3 ou ocorrerá antecipadamente caso o adjudicatário apresente a apólice antes do termo final do prazo de 1 (um) mês;

9.4.2. Caso o adjudicatário opte por outra modalidade de garantia (caução em dinheiro/títulos da dívida pública ou fiança bancária), a prestação da garantia e a convocação para a assinatura do contrato seguirão o prazo regular do item 9.2.

9.5. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do Termo de Contrato ou instrumento equivalente, a Administração poderá:

a) encaminhá-lo para assinatura, mediante correspondência postal com aviso de recebimento (AR), para que seja assinado e devolvido no prazo de 5 (cinco) dias úteis, a contar da data de seu recebimento;

b) disponibilizar acesso a sistema de processo eletrônico para que seja assinado digitalmente em até 5 (cinco) dias úteis; ou

c) outro meio eletrônico, assegurado o prazo de 5 (cinco) dias úteis para resposta após recebimento da notificação pela Administração.

9.6. Os prazos dos itens 9.2 e 9.3 poderão ser prorrogados, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

9.7. O prazo de vigência da contratação é o estabelecido no Termo de Referência.

9.8. Na assinatura do contrato ou instrumento equivalente será exigido o Cadastro Informativo de Créditos não Quitados do Setor Público Federal - Cadin e a comprovação das condições de habilitação e contratação consignadas neste Edital, que deverão ser mantidas pelo fornecedor durante a vigência do contrato.

9.8.1. A existência do registro do Cadin constitui fator impeditivo para a contratação.

10. DOS RECURSOS

10.1. A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação, observará o disposto no art. 165 da Lei nº 14.133, de 2021.

10.2. O prazo recursal é de 3 (três) dias úteis, contados da data de intimação ou de lavratura da ata.

10.3. Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do licitante:

10.3.1. a intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão;

10.3.2. o prazo para a manifestação da intenção de recorrer não será inferior a 10 (dez) minutos.

10.3.3. o prazo para apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação;

10.4. Os recursos deverão ser encaminhados em campo próprio do sistema.

10.5. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá reconsiderar sua decisão no prazo de 3 (três) dias úteis, ou, nesse mesmo prazo, encaminhar recurso para a autoridade superior, a qual deverá proferir sua

decisão no prazo de 10 (dez) dias úteis, contado do recebimento dos autos.

10.6. Os recursos interpostos fora do prazo não serão conhecidos.

10.7. O prazo para apresentação de contrarrazões ao recurso pelos demais licitantes será de 3 (três) dias úteis, contados da data da intimação pessoal ou da divulgação da interposição do recurso, assegurada a vista imediata dos elementos indispensáveis à defesa de seus interesses.

10.8. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

10.9. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

10.10. Os autos do processo poderão ser disponibilizados aos interessados por meio do e-mail: compras@crmmg.org.br.

11. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

11.1. Comete infração administrativa, nos termos da lei, o licitante que, com dolo ou culpa:

11.1.1. deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo/a Pregoeiro/a durante o certame;

11.1.2. Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta em especial quando:

11.1.2.1. não enviar a proposta adequada ao último lance ofertado ou após a negociação;

11.1.2.2. recusar-se a enviar o detalhamento da proposta quando exigível;

11.1.2.3. pedir para ser desclassificado quando encerrada a etapa competitiva;

11.1.2.4. deixar de apresentar amostra; ou

11.1.2.5. apresentar proposta ou amostra em desacordo com as especificações do edital;

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

11.1.4. recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

11.1.5. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação

11.1.6. fraudar a licitação;

11.1.7. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

11.1.7.1. agir em conluio ou em desconformidade com a lei;

11.1.7.2. induzir deliberadamente a erro no julgamento;

11.1.7.3. apresentar amostra falsificada ou deteriorada;

11.1.8. praticar atos ilícitos com vistas a frustrar os objetivos da licitação

11.1.9. praticar ato lesivo previsto no art. 5º da Lei n.º 12.846, de 2013.

11.2. Com fulcro na [Lei nº 14.133, de 2021](#), a Administração poderá, garantida a prévia defesa, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das

responsabilidades civil e criminal:

11.2.1. advertência;

11.2.2. multa;

11.2.3. impedimento de licitar e contratar e

11.2.4. declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

11.3. Na aplicação das sanções serão considerados:

11.3.1. a natureza e a gravidade da infração cometida.

11.3.2. as peculiaridades do caso concreto

11.3.3. as circunstâncias agravantes ou atenuantes

11.3.4. os danos que dela provierem para a Administração Pública

11.3.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

11.4. A multa será recolhida no prazo máximo de 15 (quinze) dias úteis, a contar da comunicação oficial.

11.4.1. Para as infrações previstas nos itens 11.1.1, 11.1.2 e 11.1.3, a multa será de 0.5% a 15% do valor do contrato licitado.

11.4.2. Para as infrações previstas nos itens 11.1.4, 11.1.5, 11.1.6, 11.1.7, 11.1.8 e 11.1.9, a multa será de 15% a 30% do valor do contrato licitado.

11.5. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.

11.6. Na aplicação da sanção de multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

11.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 11.1.1, 11.1.2 e 11.1.3, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo o qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.

11.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 11.1.5, 11.1.6, 11.1.7, 11.1.8 e 11.1.9, bem como pelas infrações administrativas previstas nos itens 11.1.1, 11.1.2, 11.1.3 e 11.1.4, que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei n.º 14.133, de 2021.

11.9. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no item 11.1.4, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação, nos termos do art. 45, §4º da IN SEGES/ME n.º 73, de 2022.

11.10. A apuração de responsabilidade relacionadas às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta por 2 (dois) ou mais

servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o adjudicatário para, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

11.11. Caberá recurso no prazo de 15 (quinze) dias úteis da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, contado da data da intimação, o qual será dirigido à autoridade que tiver proferido a decisão recorrida, que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.

11.12. Caberá a apresentação de pedido de reconsideração da aplicação da sanção de declaração de inidoneidade para licitar ou contratar no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.

11.13. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

11.14. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados.

11.15. Para a garantia da ampla defesa e contraditório dos licitantes, as notificações serão enviadas eletronicamente para os endereços de e-mail informados na proposta comercial, bem como os cadastrados pela empresa no SICAF.

11.15.1. Os endereços de e-mail informados na proposta comercial e/ou cadastrados no Sicafe serão considerados de uso contínuo da empresa, não cabendo alegação de desconhecimento das comunicações a eles comprovadamente enviadas.

12. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

12.1. Qualquer pessoa é parte legítima para impugnar este Edital por irregularidade na aplicação da Lei nº 14.133, de 2021, devendo protocolar o pedido até 3 (três) dias úteis antes da data da abertura do certame.

12.2. A resposta à impugnação ou ao pedido de esclarecimento será divulgado em sítio eletrônico oficial no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame.

12.3. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica, pelos seguintes meios: compras@crmmg.org.br

12.4. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

12.5. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo Pregoeiro, nos autos do processo de licitação.

12.6. Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

13. DAS DISPOSIÇÕES GERAIS

13.1. Será divulgada ata da sessão pública no sistema eletrônico.

13.2. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo Pregoeiro.

13.3. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília - DF.

13.4. A homologação do resultado desta licitação não implicará direito à contratação.

13.5. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

13.6. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

13.7. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.

13.8. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

13.9. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

13.10. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e endereço eletrônico <https://www.crmmg.org.br>

13.11. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

13.11.1. ANEXO I - Termo de Referência.

13.11.1.1. Apêndice do Anexo I - Estudo Técnico Preliminar

13.11.2. ANEXO II - Minuta de Contrato

Belo Horizonte, 29 de julho de 2026

.....
Matheus Tadeu da Silveira Moreira

Analista de Licitação

AGU - Advocacia Geral da União / CGU - Consultoria-Geral da União / Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União

Atualização: NOV/2025

Edital modelo para Pregão Eletrônico - Lei nº 14.133, de 2021.

Aprovado pela Secretaria de Governo Digital.



Documento assinado eletronicamente por **Lívia Pinheiro de Azevedo**, **Coordenador(a) do Setor de Compras e Licitação do CRM-MG**, em 13/08/2026, às 15:52, com fundamento no art. 5º da [RESOLUÇÃO CFM nº2.308/2022, de 28 de março de 2022](#).



A autenticidade do documento pode ser conferida no site https://sei.cfm.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **4710841** e o código CRC **BE57F3D0**.



Rua dos Timbiras, 1200 - Bairro Boa Viagem |
CEP 30140-064 | Belo Horizonte/MG -
<https://www.crmmg.org.br/>



Referência: Processo SEI nº 26.13.000003312-0 | data de inclusão: 13/08/2026



CONSELHO REGIONAL DE MEDICINA DO ESTADO DE MINAS GERAIS

TERMO DE REFERÊNCIA 14.133/21 PREGÃO/CONCORRÊNCIA Nº SEI-6 - CRM-MG/PRE/CRM-MG/PRE/DETIN

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Aquisição de Solução Integrada de Segurança da Informação, em lote único, contemplando o fornecimento, implantação, configuração, suporte técnico, garantia, licenciamento, atualizações e transferência de conhecimento, pelo período de 60 (sessenta) meses, incluindo firewalls de próxima geração, equipamento de gerenciamento centralizado, switches, access points, solução de detecção e resposta de endpoint — XDR, serviço de instalação e configuração e treinamento oficial do fabricante, conforme condições e exigências estabelecidas neste Termo de Referência e em seus anexos.

ITEM	ESPECIFICAÇÃO	CATMAT	UNIDADE DE MEDIDA	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	Equipamento de gerenciamento centralizado — appliance	618980	unidade	1	R\$ 347.094,39	R\$ 347.094,39
2	Firewall - tipo 1	609340	unidade	2	R\$ 65.644,11	R\$ 131.288,21
3	Firewall - tipo 2	609340	unidade	20	R\$ 6.327,84	R\$ 126.556,71
4	Switch gigabit de 8 portas com PoE	626423	unidade	7	R\$ 7.318,46	R\$ 51.229,20
5	Switch gigabit de 16 portas	300719	unidade	20	R\$ 13.908,39	R\$ 278.167,81
6	Access point interno - tipo 1	603936	unidade	30	R\$ 4.781,82	R\$ 143.454,72
7	Access point interno - tipo 2	603936	unidade	20	R\$ 4.069,74	R\$ 81.394,88
8	Solução de detecção e resposta de endpoint — XDR	27472	licença/unidade	330	R\$ 1.925,72	R\$ 635.485,40
9	Licenciamento, atualizações, suporte 24x7 do fabricante e garantia de 60 meses para toda a solução	27740	serviço	1	R\$ 623.941,55	R\$ 623.941,55
10	Instalação e configuração da solução	26972	serviço	1	R\$ 111.258,07	R\$ 111.258,07
11	Treinamento oficial do fabricante em cada produto fornecido, para turma de até 2 participantes	3840	serviço	1	R\$ 56.942,25	R\$ 56.942,25
Total:						R\$ 2.586.813,19

1.2. Classificação do objeto quanto à heterogeneidade ou complexidade

1.2.1. Os bens objeto desta contratação são caracterizados como comuns, porque seus padrões de desempenho, qualidade, funcionalidades e características técnicas podem ser definidos de forma objetiva neste Termo de Referência, por meio de especificações usuais de mercado, permitindo a comparação das propostas com base em critérios claros de aceitabilidade, conformidade técnica e preço.

1.3. **Classificação do objeto como bem de luxo**

1.3.1. O objeto desta contratação não se enquadra como bem de luxo, conforme Decreto nº 10.818, de 27 de setembro de 2021.

1.4. **Classificação do objeto quanto ao modelo de execução**

1.4.1. O fornecimento do objeto será integral, compreendendo a entrega dos equipamentos, licenças, subscrições e demais componentes da solução, bem como a execução dos serviços acessórios de instalação, configuração, ativação e transferência de conhecimento, sem prejuízo das obrigações de garantia, suporte técnico, atualizações, assistência técnica e manutenção da regularidade das licenças e subscrições pelo período de 60 (sessenta) meses.

1.5. **Prazo de vigência**

1.5.1. O prazo de vigência inicial da contratação é de 60 (sessenta) meses, contados do recebimento definitivo da solução, podendo ser prorrogado, observado o limite de até 10 (dez) anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021.

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

2. **FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE**

2.1. A presente contratação justifica-se pela necessidade de modernização e fortalecimento da segurança da informação no âmbito do CRM-MG, considerando a crescente dependência dos serviços institucionais em relação à infraestrutura tecnológica, à conectividade entre a Sede e as Delegacias Regionais e à proteção dos dados e sistemas corporativos.

2.2. Atualmente, a rede corporativa do CRM-MG demanda maior integração entre os mecanismos de proteção de perímetro, controle de acesso, gerenciamento de rede e proteção dos endpoints. A evolução das ameaças cibernéticas, como malwares avançados, ransomware, tentativas de acesso indevido e exploração de vulnerabilidades, exige a adoção de arquitetura de segurança mais moderna, integrada e centralizada, capaz de ampliar a visibilidade sobre o ambiente tecnológico e melhorar a capacidade de prevenção, detecção e resposta a incidentes.

2.3. A solução pretendida contempla firewalls de próxima geração, equipamento de gerenciamento centralizado, switches, access points, solução de detecção e resposta de endpoint — XDR, licenciamento, atualizações, suporte técnico, garantia, instalação, configuração e treinamento oficial do fabricante. A integração desses componentes permitirá maior controle e visibilidade sobre o ambiente tecnológico institucional, reforço à prevenção, detecção e resposta a incidentes de segurança, melhoria no controle de acessos, padronização da infraestrutura de rede e ampliação da proteção dos serviços essenciais do CRM-MG.

2.4. A contratação busca garantir maior disponibilidade, confidencialidade e integridade das informações institucionais, proteger sistemas e serviços críticos, padronizar a infraestrutura de segurança e rede, reduzir riscos operacionais e fortalecer a governança de tecnologia da informação, em alinhamento à Lei Geral de Proteção de Dados — LGPD, às normas de compliance e às boas práticas de segurança da informação aplicáveis à Administração Pública.

2.5. As quantidades estimadas foram definidas com base na necessidade de atendimento da Sede e das 20 Delegacias Regionais do CRM-MG, bem como no quantitativo estimado de endpoints a serem protegidos pela solução de detecção e resposta de endpoint

— XDR. Foram considerados, ainda, os componentes necessários ao gerenciamento centralizado, à alta disponibilidade dos recursos críticos, à padronização da infraestrutura de rede cabeada e sem fio, ao licenciamento, às atualizações, ao suporte técnico, à garantia pelo período de 60 (sessenta) meses, à instalação, à configuração e à transferência de conhecimento à equipe técnica do CRM-MG.

2.6. A contratação da Solução Integrada de Segurança da Informação está prevista no Plano Anual de Compras do CRM-MG, conforme indicado no Documento de Oficialização da Demanda, que registra a previsão de aquisição para julho de 2026.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO

3.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

3.2. A solução de TIC consiste na aquisição de Solução Integrada de Segurança da Informação, em lote único, contemplando o fornecimento de equipamentos físicos, licenças de software, subscrições, suporte técnico, garantia, atualizações, instalação, configuração e treinamento oficial do fabricante.

3.3. A solução abrange o fornecimento de firewalls de próxima geração, equipamento de gerenciamento centralizado, switches, access points e solução de detecção e resposta de endpoint — XDR, devendo os componentes serem do mesmo fabricante e possuir compatibilidade técnica e capacidade de operação integrada, de forma a permitir a padronização da infraestrutura de segurança e rede, o gerenciamento centralizado, a aplicação uniforme de políticas de segurança, a proteção dos endpoints e a ampliação da capacidade de prevenção, detecção e resposta a incidentes de segurança da informação.

3.4. A contratação envolve itens de naturezas diversas, compreendendo bens de TIC, licenças, subscrições e serviços acessórios de instalação, configuração, suporte, garantia e treinamento, os quais se integram para atender à necessidade institucional do CRM-MG. A solução deverá ser entregue de forma completa, funcional, integrada, licenciada, atualizada, suportada e garantida durante todo o período contratado.

3.5. Todos os equipamentos e softwares fornecidos deverão ser novos, de primeiro uso, originais de fábrica, próprios para uso corporativo e não poderão estar descontinuados, em fim de comercialização, em fim de suporte e/ou em fim de vida útil nos próximos 36 meses na data de apresentação da proposta, observadas as demais especificações técnicas constantes deste Termo de Referência e de seus anexos.

3.6. O ciclo de vida do objeto envolve as fases de fornecimento, implantação, operação, suporte, manutenção, atualização, garantia, transferência de conhecimento e, quando aplicável, desfazimento ou substituição ambientalmente adequada dos equipamentos.

3.7. Na fase de fornecimento, deverão ser entregues os equipamentos, licenças, subscrições, acessórios, documentação técnica e demais componentes necessários ao funcionamento da solução.

3.8. Na fase de implantação, a Contratada será responsável pela instalação, configuração, integração, testes, validações e ativação da solução no ambiente tecnológico do CRM-MG, devendo adotar medidas para minimizar impactos na rede em funcionamento e preservar a continuidade dos serviços institucionais.

3.9. Na fase de operação e manutenção, a solução deverá contar com suporte técnico, licenciamento, atualizações e garantia pelo período de 60 (sessenta) meses, incluindo correções, atualizações de firmware e software, substituição de componentes defeituosos e demais providências necessárias à manutenção da disponibilidade, segurança e integridade da solução.

3.10. A transferência de conhecimento deverá ocorrer por meio de treinamento oficial do fabricante, destinado à equipe técnica do CRM-MG, contemplando conteúdo compatível com os produtos fornecidos e com as necessidades de administração, operação e

acompanhamento da solução.

3.11. Quanto ao desfazimento ou substituição de componentes, deverão ser observadas as diretrizes de sustentabilidade aplicáveis, especialmente quanto à eficiência energética, durabilidade, redução da geração de resíduos eletroeletrônicos, descarte ambientalmente adequado e logística reversa, quando cabível.

4. REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos de Negócio

4.1.1. A presente contratação orienta-se pelos seguintes requisitos de negócio:

4.1.1.1. fortalecer a segurança da informação no âmbito do CRM-MG, mediante a implantação de solução integrada capaz de ampliar a proteção da infraestrutura tecnológica, dos dados institucionais e dos sistemas corporativos;

4.1.1.2. reduzir riscos operacionais e de segurança decorrentes de soluções heterogêneas, desatualizadas ou de difícil gerenciamento, promovendo maior padronização da infraestrutura de segurança e rede;

4.1.1.3. permitir o gerenciamento centralizado dos componentes da solução, com aplicação uniforme de políticas de segurança, maior visibilidade do ambiente tecnológico e melhoria da capacidade de acompanhamento e resposta a eventos e incidentes;

4.1.1.4. proteger a infraestrutura tecnológica da Sede e das Delegacias Regionais do CRM-MG, contemplando recursos de proteção de perímetro, conectividade cabeada, conectividade sem fio e proteção dos endpoints;

4.1.1.5. ampliar a capacidade de prevenção, detecção e resposta a ameaças cibernéticas, incluindo malwares, ransomware, acessos indevidos, exploração de vulnerabilidades e comportamentos suspeitos;

4.1.1.6. contribuir para a continuidade dos serviços institucionais suportados pela infraestrutura tecnológica, reduzindo riscos de indisponibilidade, falhas de segurança e impactos às atividades administrativas e finalísticas do CRM-MG;

4.1.1.7. apoiar a governança de tecnologia da informação e segurança da informação, mediante recursos de registro, auditoria, rastreabilidade, controle de acessos e visibilidade sobre o ambiente tecnológico;

4.1.1.8. contribuir para a conformidade com a Lei Geral de Proteção de Dados — LGPD, normas de compliance e boas práticas de segurança da informação aplicáveis à Administração Pública;

4.1.1.9. assegurar suporte técnico, licenciamento, atualizações e garantia pelo período contratado, de modo a preservar a continuidade, a disponibilidade, a integridade e a confidencialidade dos serviços e informações institucionais;

4.1.1.10. possibilitar a transferência de conhecimento à equipe técnica do CRM-MG, permitindo melhor acompanhamento, administração e operação dos principais recursos da solução.

4.2. Requisitos de Capacitação

4.2.1. Será necessário treinamento à equipe que atuará com a solução.

4.2.2. O treinamento deverá ser oficial do fabricante, contemplando todos os produtos fornecidos na solução, incluindo, no mínimo, os recursos necessários à administração, operação, monitoramento, atualização, suporte inicial, aplicação de políticas, consulta de logs, análise de eventos e acompanhamento dos principais recursos da solução.

4.2.3. O treinamento deverá abranger os componentes relevantes da solução integrada, incluindo firewalls de próxima geração, equipamento de gerenciamento centralizado, switches, access points e solução de detecção e resposta de endpoint — XDR, observadas as características dos produtos efetivamente ofertados.

4.2.4. O treinamento deverá ser destinado a uma turma de até 2 (dois) participantes indicados pelo CRM-MG, podendo ser realizado de forma presencial, remota ou em ambiente oficial de treinamento disponibilizado pelo fabricante, desde que assegurada a efetiva transferência de conhecimento à equipe técnica da Contratante.

4.2.5. A capacitação deverá ocorrer preferencialmente após a implantação e configuração da solução, ou em momento previamente acordado com a Contratante que permita melhor aproveitamento prático do conteúdo ministrado.

4.2.6. A Contratada deverá disponibilizar, quando for o caso e sem ônus adicional, materiais didáticos, manuais, documentação técnica, certificados ou comprovantes de participação, quando aplicáveis, bem como as informações necessárias para acesso ao ambiente de treinamento.

4.3. Requisitos Legais

4.3.1. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133, de 1º de abril de 2021, à Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, à Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, à Lei nº 13.709, de 14 de agosto de 2018 — Lei Geral de Proteção de Dados Pessoais (LGPD), à Lei nº 12.527, de 18 de novembro de 2011 — Lei de Acesso à Informação, à Lei nº 12.305, de 2 de agosto de 2010 — Política Nacional de Resíduos Sólidos, ao Decreto nº 10.240, de 12 de fevereiro de 2020, e às demais legislações e normas aplicáveis.

4.3.2. A solução deverá observar, ainda, no que couber, as normas de segurança da informação, proteção de dados pessoais, governança de tecnologia da informação, acessibilidade, sustentabilidade, descarte ambientalmente adequado de resíduos eletroeletrônicos, logística reversa, bem como as normas técnicas e regulatórias aplicáveis aos equipamentos, softwares, licenças e serviços que compõem a contratação.

4.3.3. Quando aplicável, os equipamentos deverão atender às exigências de homologação, certificação ou conformidade técnica exigidas pelos órgãos reguladores competentes, especialmente em relação aos componentes de conectividade sem fio e demais equipamentos sujeitos à regulamentação da Agência Nacional de Telecomunicações — ANATEL.

4.3.4. A execução contratual deverá observar, ainda, a Política de Segurança da Informação, as normas internas e os procedimentos institucionais do CRM-MG aplicáveis ao acesso, tratamento, armazenamento, compartilhamento e proteção das informações institucionais.

4.4. Requisitos de Manutenção

4.4.1. Devido às características da solução, há necessidade de manutenção da disponibilidade, atualização, segurança e adequado funcionamento dos componentes contratados durante todo o período de vigência, especialmente em razão da criticidade da infraestrutura de segurança da informação para a continuidade dos serviços institucionais do CRM-MG.

4.4.2. A solução deverá contar com mecanismos de suporte, atualização, correção e recomposição de funcionamento em caso de falhas, de modo a preservar a proteção da rede corporativa, dos endpoints, da conectividade e dos sistemas institucionais.

4.4.3. Os requisitos específicos relativos à garantia, manutenção, assistência técnica, suporte, substituição de componentes, prazos de atendimento e demais condições operacionais serão tratados em item próprio deste Termo de Referência.

4.5. Requisitos Temporais

4.5.1. A entrega dos equipamentos, licenças, subscrições e demais componentes necessários à solução deverá ser efetivada no prazo máximo de 90 (noventa) dias corridos, contado do recebimento da Ordem de Fornecimento de Bens — OFB emitida pela

Contratante.

4.5.2. As etapas de implantação, configuração, integração, testes, validações e ativação da solução deverão observar cronograma a ser apresentado pela Contratada e aprovado pela Contratante, considerando as condições de execução previstas neste Termo de Referência e em seus anexos.

4.5.3. Os serviços deverão ser planejados e executados de forma a minimizar impactos no ambiente tecnológico em funcionamento, devendo eventuais intervenções que possam gerar indisponibilidade, degradação de desempenho ou alteração relevante no ambiente ser previamente comunicadas e autorizadas pela Contratante.

4.5.4. Na contagem dos prazos estabelecidos neste Termo de Referência, quando não expressamente indicado de forma diversa, excluir-se-á o dia do início e incluir-se-á o dia do vencimento.

4.5.5. Todos os prazos citados, quando não expressos de forma diversa, serão considerados em dias corridos.

4.6. Requisitos de Segurança e Privacidade

4.6.1. A solução deverá atender aos princípios e procedimentos de segurança da informação, proteção de dados pessoais, confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade aplicáveis ao ambiente tecnológico do CRM-MG.

4.6.2. Todas as informações, documentos, dados, configurações, registros, credenciais, diagramas, políticas de segurança, parâmetros técnicos e demais elementos aos quais a Contratada tiver acesso em razão da execução contratual deverão ser tratados como confidenciais, sendo vedada sua reprodução, utilização, compartilhamento ou divulgação a terceiros sem autorização expressa da Contratante.

4.6.3. A Contratada deverá adotar medidas técnicas, administrativas e operacionais adequadas para proteger as informações institucionais do CRM-MG contra acessos não autorizados, perda, alteração, divulgação indevida, uso inadequado ou qualquer forma de tratamento incompatível com a finalidade da contratação.

4.6.4. A Contratada não poderá utilizar a presente contratação para obter acesso não autorizado a informações, sistemas, ambientes, redes, bases de dados ou quaisquer recursos tecnológicos do CRM-MG.

4.6.5. Os acessos concedidos à Contratada deverão observar o princípio do menor privilégio, limitando-se ao estritamente necessário para a execução do objeto, pelo tempo necessário e mediante autorização da Contratante.

4.6.6. Quando houver necessidade de acesso remoto ao ambiente tecnológico do CRM-MG, este deverá ser previamente autorizado e realizado por meio definido pela Contratante, preferencialmente com acompanhamento de representante técnico do CRM-MG.

4.6.7. A Contratada deverá comunicar imediatamente à Contratante qualquer incidente, vulnerabilidade, exposição indevida de informações, tentativa de acesso não autorizado ou evento que possa comprometer a segurança, a privacidade, a disponibilidade ou a integridade da solução ou dos dados institucionais.

4.6.8. A Contratada não poderá manter, reter ou armazenar, sem autorização expressa da Contratante, cópias de documentos técnicos, configurações, credenciais, registros, bases de dados ou quaisquer informações institucionais às quais tenha tido acesso em razão da execução contratual.

4.6.9. Os profissionais da Contratada que atuarem direta ou indiretamente na execução do objeto deverão observar as normas de segurança da informação, privacidade e sigilo aplicáveis, bem como assinar os instrumentos de compromisso e ciência previstos neste Termo de Referência, quando exigidos.

4.6.10. A execução contratual deverá observar a Lei Geral de Proteção de Dados Pessoais — LGPD, a Lei de Acesso à Informação — LAI, as normas internas do CRM-MG e as demais disposições legais e regulamentares aplicáveis à proteção das informações institucionais.

4.7. Requisitos Sociais, Ambientais e Culturais

4.7.1. Os equipamentos, licenças, serviços de suporte, garantia, instalação, configuração, treinamento e demais componentes da solução deverão observar, no que couber, requisitos sociais, ambientais e culturais compatíveis com a natureza do objeto e com as diretrizes institucionais do CRM-MG.

4.7.2. O atendimento, suporte técnico, treinamento, documentação operacional, comunicações formais e demais interações necessárias à execução contratual deverão ocorrer em língua portuguesa do Brasil, admitida documentação técnica complementar em língua inglesa quando usual no mercado de tecnologia da informação e segurança da informação.

4.7.3. Os materiais de treinamento, manuais, orientações técnicas e demais documentos de apoio deverão ser apresentados, quando for o caso, de forma clara e compatível com a adequada transferência de conhecimento à equipe técnica do CRM-MG.

4.7.4. A Contratada deverá pautar sua atuação pelo uso racional de recursos, evitando desperdício de insumos, materiais, embalagens e demais recursos consumidos na execução contratual.

4.7.5. A Contratada deverá observar práticas ambientalmente adequadas na execução do objeto, especialmente quanto ao acondicionamento, transporte, instalação, substituição e eventual descarte de equipamentos, componentes, peças, embalagens e resíduos eletroeletrônicos, quando aplicável.

4.7.6. Os profissionais, prepostos ou colaboradores da Contratada que atuarem nas dependências do CRM-MG deverão observar as normas internas, identificar-se quando solicitado, manter conduta compatível com o ambiente institucional e evitar interferências indevidas nas atividades da Contratante.

4.7.7. A Contratada deverá assumir integral responsabilidade pelos encargos e obrigações sociais, trabalhistas, previdenciárias, fiscais e comerciais decorrentes da execução contratual, não se estabelecendo qualquer vínculo empregatício entre seus profissionais, prepostos ou colaboradores e o CRM-MG.

4.7.8. A execução contratual deverá respeitar as normas de segurança e saúde ocupacional aplicáveis às atividades desempenhadas pela Contratada, especialmente quando houver atuação presencial nas dependências do CRM-MG.

4.8. Requisitos da Arquitetura Tecnológica

4.8.1. A solução deverá adotar arquitetura integrada, centralizada e multicamadas de segurança da informação e infraestrutura de rede, contemplando recursos de proteção de perímetro, gerenciamento centralizado, conectividade cabeada, conectividade sem fio, proteção de endpoints, registro de eventos, auditoria e resposta a incidentes.

4.8.2. A arquitetura tecnológica deverá possibilitar a operação integrada dos componentes fornecidos, incluindo firewalls de próxima geração, equipamento de gerenciamento centralizado, switches, access points e solução de detecção e resposta de endpoint — XDR, de forma a permitir maior visibilidade, controle, correlação de eventos, aplicação uniforme de políticas de segurança e resposta coordenada a incidentes.

4.8.3. A arquitetura deverá contemplar alta disponibilidade para os componentes críticos instalados no CRM-MG, especialmente quanto aos firewalls de próxima geração destinados ao ambiente central, de modo a reduzir riscos de indisponibilidade dos serviços institucionais suportados pela infraestrutura tecnológica.

- 4.8.4. A solução deverá permitir gerenciamento centralizado dos componentes, possibilitando a administração, configuração, monitoramento, aplicação de políticas, consulta de registros, auditoria, atualização, acompanhamento de eventos e extração de informações necessárias à gestão da segurança da informação.
- 4.8.5. A solução deverá favorecer a visibilidade consolidada do ambiente de segurança e rede, permitindo à equipe técnica do CRM-MG acompanhar, em interface ou ferramenta centralizada, o estado dos principais componentes, eventos relevantes, alertas, registros e indicadores operacionais da solução.
- 4.8.6. A solução deverá permitir, quando aplicável, a administração por perfis de acesso, de forma a possibilitar segregação de funções, controle de permissões, rastreabilidade de ações administrativas e redução de riscos decorrentes de privilégios excessivos.
- 4.8.7. Os componentes da solução deverão possuir compatibilidade técnica entre si e com o ambiente tecnológico do CRM-MG, de modo a permitir implantação, operação, manutenção, atualização, suporte, expansão e substituição de componentes de forma adequada durante todo o período contratado.
- 4.8.8. A solução deverá possuir capacidade de interoperar com o ambiente tecnológico existente do CRM-MG, observadas as especificações técnicas deste Termo de Referência, de modo a permitir sua implantação sem necessidade de substituições não previstas, adaptações excessivas ou dependências incompatíveis com a infraestrutura institucional.
- 4.8.9. A arquitetura deverá permitir a aplicação de atualizações, correções e melhorias de forma controlada, planejada e compatível com os componentes da solução, de modo a preservar a estabilidade, a segurança e a continuidade do ambiente tecnológico.
- 4.8.10. A arquitetura deverá permitir a proteção integrada contra ameaças modernas, incluindo, no que couber, malwares, ransomware, acessos indevidos, exploração de vulnerabilidades, tráfego malicioso, comportamentos suspeitos e demais eventos que possam comprometer a segurança, a disponibilidade, a integridade ou a confidencialidade das informações institucionais.
- 4.8.11. A solução deverá possibilitar a integração entre os recursos de segurança de perímetro, rede interna, rede sem fio e endpoints, permitindo maior capacidade de prevenção, detecção, correlação, investigação e resposta a eventos e incidentes de segurança.
- 4.8.12. A solução deverá permitir o registro, a consulta, a análise e a auditoria de logs e eventos relacionados aos componentes contratados, de forma a subsidiar ações de monitoramento, investigação, conformidade, rastreabilidade e resposta a incidentes de segurança da informação.
- 4.8.13. A arquitetura deverá favorecer a segmentação, o controle de acessos, a aplicação de políticas de segurança e a visibilidade sobre o tráfego de rede, observadas as características e limitações técnicas dos componentes efetivamente contratados.
- 4.8.14. A eventual indisponibilidade temporária de comunicação entre componentes remotos e o ambiente de gerenciamento centralizado não deverá impedir o funcionamento básico dos recursos locais de conectividade e segurança previamente configurados, observadas as características técnicas da solução ofertada.
- 4.8.15. Os equipamentos, softwares, licenças, subscrições e demais componentes deverão ser dimensionados para atender às necessidades atuais do CRM-MG, bem como permitir expansão, atualização tecnológica e continuidade operacional durante o ciclo de vida da contratação.
- 4.8.16. Os componentes fornecidos não poderão estar descontinuados, em fim de comercialização, em fim de suporte ou em fim de vida útil na data de apresentação da proposta, devendo possuir ciclo de vida compatível com o prazo de suporte, licenciamento, atualização e garantia exigido neste Termo de Referência.

4.8.17. A solução deverá ser concebida de forma a evitar dependência de componentes isolados ou incompatíveis entre si, assegurando que os itens fornecidos funcionem de maneira integrada e coerente com a finalidade da contratação.

4.8.18. Os requisitos técnicos específicos de cada componente da solução serão detalhados no Anexo de Especificações Técnicas deste Termo de Referência.

4.9. Requisitos de Projeto e de Implementação

4.9.1. A Contratada deverá planejar a implementação da solução de forma organizada, documentada e compatível com o ambiente tecnológico do CRM-MG, observando as condições estabelecidas neste Termo de Referência, em seus anexos e nas orientações da equipe técnica da Contratante.

4.9.2. Antes do início das atividades técnicas, a Contratada deverá realizar, em conjunto com a equipe técnica do CRM-MG, o levantamento das informações necessárias à adequada configuração, parametrização, integração, testes e preparação da solução, respeitados os limites de acesso, confidencialidade e segurança definidos pela Contratante.

4.9.3. A Contratada deverá apresentar plano ou cronograma de implementação da solução, contendo, no mínimo, as etapas previstas, atividades principais, responsabilidades, dependências, prazos estimados, riscos operacionais relevantes, janelas de execução, procedimentos de validação e, quando aplicável, plano de reversão ou contingência para mudanças críticas.

4.9.4. O plano ou cronograma de implementação deverá ser previamente analisado e aprovado pela Contratante antes da execução das atividades que possam impactar o ambiente tecnológico do CRM-MG.

4.9.5. O projeto de implementação deverá considerar a infraestrutura tecnológica existente no CRM-MG, buscando reduzir impactos operacionais, evitar interrupções indevidas, preservar a continuidade dos serviços institucionais e assegurar compatibilidade com os recursos atualmente em funcionamento.

4.9.6. A implementação poderá ser planejada de forma faseada ou por etapas, conforme aprovação da Contratante, de modo a permitir validação gradual dos componentes, redução de riscos operacionais e melhor acompanhamento pela equipe técnica do CRM-MG.

4.9.7. As atividades que possam gerar indisponibilidade, degradação de desempenho, alteração relevante de configuração, impacto na conectividade, nos serviços de rede, nos endpoints ou nos mecanismos de segurança deverão ser previamente comunicadas e executadas somente em janelas autorizadas pela Contratante.

4.9.8. A Contratada deverá prever procedimentos técnicos que permitam a adequada integração dos componentes da solução, incluindo firewalls de próxima geração, equipamento de gerenciamento centralizado, switches, access points e solução de detecção e resposta de endpoint — XDR, observadas as especificações técnicas deste Termo de Referência e de seus anexos.

4.9.9. O planejamento da implementação deverá contemplar os testes necessários para comprovar a adequada configuração, integração, comunicação, gerenciamento, atualização e funcionamento dos componentes, bem como a aplicação das políticas e funcionalidades essenciais definidas para a solução.

4.9.10. Os procedimentos de teste e validação deverão contemplar, quando aplicável, conectividade, gerenciamento centralizado, comunicação entre componentes, registro de logs e eventos, aplicação de políticas de segurança, atualização dos componentes, funcionamento dos recursos de proteção, administração da solução e demais funcionalidades necessárias à operação inicial.

4.9.11. Durante a execução das atividades técnicas, eventuais ajustes relevantes, decisões de configuração, alterações em relação ao planejamento inicial ou ocorrências que

possam impactar o funcionamento da solução deverão ser registrados e comunicados à equipe técnica do CRM-MG, de modo a subsidiar a documentação final da solução.

4.9.12. A Contratada deverá prestar orientações operacionais iniciais à equipe técnica do CRM-MG sobre as atividades técnicas realizadas e sobre os principais parâmetros definidos para a solução, sem prejuízo do treinamento oficial do fabricante previsto neste Termo de Referência.

4.10. Requisitos de Implantação

4.10.1. A implantação da solução deverá ser executada pela Contratada, sob acompanhamento da equipe técnica do CRM-MG, observadas as condições estabelecidas neste Termo de Referência, em seus anexos e no plano ou cronograma previamente aprovado pela Contratante.

4.10.2. A implantação deverá contemplar, no que couber, a disponibilização dos equipamentos, licenças, subscrições, acessos, atualizações, configurações, integrações, testes, validações e demais providências necessárias ao funcionamento inicial da solução no ambiente tecnológico do CRM-MG.

4.10.3. A Contratada deverá executar as atividades de configuração, parametrização, integração e ativação dos componentes da solução, incluindo firewalls de próxima geração, equipamento de gerenciamento centralizado, switches, access points e solução de detecção e resposta de endpoint — XDR, conforme as especificações técnicas deste Termo de Referência e de seus anexos.

4.10.4. A Contratada permanecerá responsável pela adequada configuração, integração, ativação e validação técnica dos componentes da solução, ainda que determinadas atividades logísticas ou operacionais sejam realizadas pela Contratante, conforme planejamento aprovado.

4.10.5. As atividades que possam impactar a disponibilidade, o desempenho, a conectividade, os serviços de rede, os endpoints ou os mecanismos de segurança do CRM-MG deverão ser executadas em janelas previamente autorizadas pela Contratante.

4.10.6. A implantação deverá ser conduzida de forma a preservar, sempre que possível, a continuidade dos serviços institucionais, sendo vedada a realização de alterações que possam gerar interrupção relevante, degradação de desempenho ou indisponibilidade sem autorização prévia da Contratante.

4.10.7. A Contratada deverá realizar os testes necessários para comprovar o funcionamento adequado dos componentes implantados, incluindo, quando aplicável, conectividade, comunicação com o gerenciamento centralizado, aplicação de políticas de segurança, registro de logs e eventos, atualização dos componentes, funcionamento dos recursos de proteção e administração da solução.

4.10.8. Eventuais falhas, inconsistências, incompatibilidades ou pendências identificadas durante a implantação deverão ser corrigidas pela Contratada, sem ônus adicional à Contratante, antes da conclusão da etapa correspondente.

4.10.9. A Contratada deverá comprovar a ativação das licenças, subscrições, garantias, atualizações e suporte técnico vinculados à solução, observados os prazos e condições estabelecidos neste Termo de Referência e em seus anexos.

4.10.10. Ao final da implantação, a Contratada deverá disponibilizar documentação técnica da solução, contendo, no mínimo, informações sobre componentes instalados, versões, licenças, configurações relevantes, políticas aplicadas, integrações realizadas, topologia lógica, procedimentos básicos de administração, registros de testes e demais informações necessárias à operação e acompanhamento da solução pela equipe técnica do CRM-MG.

4.10.11. A Contratada deverá prestar apoio técnico inicial à equipe do CRM-MG durante a entrada em operação da solução, de modo a auxiliar na verificação do funcionamento dos

componentes, no acompanhamento de eventos e na estabilização inicial do ambiente.

4.10.12. A conclusão da implantação não substitui os procedimentos formais de recebimento provisório e definitivo, que deverão observar os critérios e etapas definidos em item próprio deste Termo de Referência.

4.10.13. A implantação somente será considerada concluída após a realização dos testes, validações e demais verificações técnicas necessárias, com aceite da Contratante, observados os critérios de recebimento definidos neste Termo de Referência.

4.11. Requisitos de Garantia, Manutenção e Assistência Técnica

4.11.1. A solução deverá contar com garantia, manutenção, atualizações, suporte técnico, licenciamento e assistência técnica pelo período de 60 (sessenta) meses, contado da emissão do Termo de Recebimento Definitivo da solução, sem prejuízo das obrigações da Contratada durante as fases de entrega, instalação, configuração, implantação, testes, validações e recebimento provisório.

4.11.2. A Contratada será integralmente responsável por assegurar a cobertura de garantia, suporte técnico, licenciamento, atualizações e demais serviços vinculados à solução durante todo o período de 60 (sessenta) meses contado do Termo de Recebimento Definitivo, ainda que tais obrigações sejam executadas, total ou parcialmente, pelo fabricante ou por sua rede autorizada.

4.11.3. A eventual negativa, limitação, descontinuidade ou restrição imposta pelo fabricante não afastará a responsabilidade da Contratada perante o CRM-MG, cabendo-lhe adotar todas as providências necessárias para garantir a plena execução contratual, sem ônus adicional à Contratante.

4.11.4. A garantia deverá abranger os equipamentos, softwares, licenças, subscrições, atualizações, componentes, acessórios e demais itens fornecidos, incluindo correção de falhas, defeitos, inconsistências, mau funcionamento, incompatibilidades e demais ocorrências que comprometam a adequada operação da solução.

4.11.5. A manutenção e a assistência técnica deverão contemplar, quando aplicável, diagnóstico, correção de falhas, substituição de peças, componentes ou equipamentos defeituosos, atualização de firmware e software, aplicação de correções, orientações técnicas e demais providências necessárias à restauração e preservação do funcionamento da solução.

4.11.6. A Contratada deverá assegurar que todos os equipamentos, licenças, subscrições, garantias, atualizações e serviços de suporte ofertados estejam devidamente registrados, habilitados ou contratados junto ao fabricante, com cobertura compatível com o prazo de 60 (sessenta) meses contado do Termo de Recebimento Definitivo da solução e com as demais condições exigidas neste Termo de Referência.

4.11.7. A solução deverá permanecer apta a receber atualizações de segurança, correções, melhorias, assinaturas, bases de inteligência de ameaças e demais recursos necessários à manutenção da proteção, estabilidade e eficácia da solução durante todo o período de garantia, suporte, licenciamento e atualização contratado.

4.11.8. Os componentes fornecidos não poderão estar descontinuados, em fim de comercialização, em fim de suporte ou em fim de vida útil pelos próximos 36 meses na data de apresentação da proposta, devendo possuir ciclo de vida compatível com o prazo de suporte, licenciamento, atualização e garantia exigido neste Termo de Referência.

4.11.9. Caso algum componente da solução venha a ser declarado em fim de comercialização, fim de suporte, fim de vida útil ou condição equivalente durante a vigência contratual, a Contratada deverá assegurar sua substituição, atualização ou evolução tecnológica por componente equivalente ou superior, compatível com a solução contratada, sem prejuízo da continuidade operacional e sem ônus adicional à Contratante, quando tal condição comprometer o atendimento aos requisitos contratados.

4.11.10. O suporte técnico, a manutenção e a assistência técnica deverão ser prestados por profissionais com conhecimento compatível com os produtos e tecnologias fornecidos, devendo abranger os componentes da solução integrada, incluindo firewalls de próxima geração, equipamento de gerenciamento centralizado, switches, access points e solução de detecção e resposta de endpoint — XDR, observados os requisitos de experiência profissional e formação da equipe previstos neste Termo de Referência.

4.11.11. A substituição dos profissionais indicados pela Contratada durante a execução contratual deverá preservar qualificação compatível com a exigida, podendo a Contratante solicitar, a qualquer tempo, a comprovação da capacidade técnica dos profissionais envolvidos no atendimento, suporte, manutenção ou assistência técnica da solução.

4.11.12. A Contratada deverá disponibilizar canais de atendimento para abertura, acompanhamento e encerramento de chamados técnicos, permitindo o registro das ocorrências, prazos, providências adotadas, responsáveis pelo atendimento e solução aplicada.

4.11.13. Os chamados técnicos deverão ser classificados conforme criticidade, impacto e urgência, observados os níveis mínimos de serviço, prazos de atendimento, prazos de solução ou demais condições estabelecidas neste Termo de Referência, em seus anexos ou no contrato.

4.11.14. A Contratada deverá manter histórico dos chamados técnicos, atendimentos, substituições, atualizações, correções e demais intervenções realizadas na solução, disponibilizando tais registros à Contratante sempre que solicitado.

4.11.15. A substituição de peças, componentes ou equipamentos defeituosos deverá ocorrer por itens novos, originais, compatíveis e de características iguais ou superiores aos originalmente fornecidos, sem ônus adicional à Contratante.

4.11.16. A Contratada deverá assegurar que eventuais substituições, correções ou atualizações não impliquem perda de funcionalidades, redução de desempenho, incompatibilidade com a solução implantada ou diminuição do nível de proteção originalmente contratado.

4.11.17. A Contratada deverá manter a solução em condições adequadas de funcionamento, segurança, atualização e suporte durante todo o período contratado, respondendo por falhas decorrentes de defeitos, incompatibilidades, vícios, ausência de atualização, indisponibilidade de suporte ou descumprimento das condições de garantia.

4.11.18. As atividades de manutenção, atualização ou assistência técnica que possam gerar indisponibilidade, degradação de desempenho ou alteração relevante no ambiente tecnológico do CRM-MG deverão ser previamente comunicadas e autorizadas pela Contratante, preferencialmente em janela de manutenção acordada entre as partes.

4.11.19. A Contratada deverá orientar a Contratante quanto à aplicação de atualizações críticas, correções de segurança, recomendações do fabricante e demais medidas necessárias à preservação da segurança e estabilidade da solução, especialmente quando envolverem riscos relevantes ao ambiente tecnológico.

4.11.20. A garantia, manutenção e assistência técnica não afastam a responsabilidade da Contratada pelo correto fornecimento, implantação, configuração, integração e funcionamento da solução, nem limitam os direitos da Contratante previstos na legislação aplicável e neste Termo de Referência.

4.12. Regularidade da solução ofertada e vínculo oficial com o fabricante

4.12.1. A Contratada deverá comprovar, por meio de documentação idônea, que possui vínculo comercial, parceria, credenciamento, autorização, certificação de canal ou condição equivalente junto ao fabricante da solução ofertada, apta a assegurar a comercialização regular dos produtos, o fornecimento das licenças e subscrições, a ativação das garantias, o acesso às atualizações e ao suporte técnico oficial, bem como a execução das atividades de implantação, configuração e suporte da solução.

4.12.2. A comprovação poderá ocorrer mediante certificado de parceria, consulta a portal oficial do fabricante, declaração do fabricante, documento de credenciamento, identificação de canal autorizado, contrato de parceria, registro de licenciamento, entitlement ou outro documento idôneo equivalente que demonstre a regularidade da relação da licitante com o fabricante da solução ofertada.

4.12.3. A exigência prevista neste item não se confunde com carta de solidariedade do fabricante, permanecendo a Contratada, conforme a fase da contratação, integralmente responsável pelo fornecimento, implantação, configuração, suporte técnico, garantia, atualizações, licenciamento e demais obrigações assumidas perante o CRM-MG.

4.13. Requisitos de Experiência Profissional

4.13.1. A Contratada deverá disponibilizar profissionais com experiência compatível com a natureza, complexidade e criticidade da solução contratada, especialmente nas atividades de implementação, implantação, configuração, integração, suporte técnico, manutenção e assistência técnica dos componentes fornecidos.

4.13.2. A experiência profissional deverá guardar relação com os produtos, tecnologias e atividades abrangidas pela contratação, incluindo, quando aplicável, firewalls de próxima geração, gerenciamento centralizado de segurança, switches, access points, solução de detecção e resposta de endpoint — XDR, redes corporativas, segurança da informação, atualização de sistemas e atendimento técnico especializado.

4.13.3. A experiência profissional exigida deverá ser compatível com a natureza da solução contratada, não se exigindo, salvo justificativa técnica específica, atuação prévia em ambiente idêntico ao da Contratante ou com os mesmos modelos de equipamentos e softwares ofertados, desde que demonstrada capacidade técnica suficiente para execução das atividades previstas.

4.13.4. A Contratada deverá comprovar, antes do início das atividades técnicas correspondentes, que dispõe de equipe com experiência compatível para atendimento à solução ofertada.

4.13.5. A indicação de profissionais experientes ou qualificados não afasta a responsabilidade integral da Contratada pela execução do objeto, pela coordenação da equipe técnica, pela qualidade dos serviços prestados e pelo pleno funcionamento da solução, independentemente de eventual participação de fabricante, distribuidor, parceiro autorizado ou equipe terceirizada.

4.13.6. A substituição dos profissionais indicados pela Contratada durante a execução contratual deverá preservar experiência compatível com as atividades a serem desempenhadas, podendo a Contratante solicitar, a qualquer tempo, a comprovação da capacidade técnica dos profissionais envolvidos na implementação, implantação, atendimento, suporte, manutenção ou assistência técnica da solução.

4.14. Requisitos de Formação da Equipe

4.14.1. A Contratada deverá disponibilizar equipe técnica com formação, capacitação e certificação oficial do fabricante compatível com a natureza, complexidade e criticidade da solução contratada, observadas as atividades a serem desempenhadas na implementação, implantação, configuração, integração, suporte técnico, manutenção e assistência técnica dos componentes fornecidos.

4.14.2. A formação da equipe deverá guardar relação com os produtos, tecnologias e atividades abrangidas pela contratação, incluindo, quando aplicável, firewalls de próxima geração, gerenciamento centralizado de segurança, switches, access points, solução de detecção e resposta de endpoint — XDR, redes corporativas, segurança da informação, atualização de sistemas e atendimento técnico especializado.

4.14.3. A Contratada deverá comprovar, antes do início das atividades técnicas correspondentes, conforme o caso, que dispõe de profissionais com capacitação compatível

para atendimento à solução ofertada, mediante apresentação de certificado oficial emitidos pelo fabricante.

4.14.4. Quando os produtos fornecidos exigirem atuação técnica especializada do fabricante, distribuidor, parceiro autorizado ou equipe certificada, caberá à Contratada assegurar a disponibilidade desses recursos durante a execução contratual, sem prejuízo de sua responsabilidade integral perante o CRM-MG.

4.14.5. A alocação da equipe não implica vínculo empregatício entre os profissionais da Contratada e o CRM-MG, nem afasta a responsabilidade da Contratada pela coordenação da equipe técnica, pela qualidade dos serviços prestados e pelo pleno funcionamento da solução.

4.14.6. A substituição de profissionais durante a execução contratual deverá preservar formação da equipe, em termos de capacitação e certificação compatível com as atividades a serem desempenhadas, podendo a Contratante solicitar, a qualquer tempo, a comprovação da qualificação técnica dos profissionais envolvidos.

4.15. Requisitos de Metodologia de Trabalho

4.15.1. O fornecimento dos equipamentos, licenças, subscrições e demais componentes da solução está condicionado ao recebimento, pela Contratada, de Ordem de Fornecimento de Bens — OFB emitida pela Contratante.

4.15.2. A OFB indicará, conforme o caso, os itens a serem fornecidos, as respectivas quantidades, os prazos aplicáveis, o local de entrega e demais informações necessárias ao adequado cumprimento da obrigação de fornecimento.

4.15.3. Os equipamentos, licenças, subscrições e demais componentes da solução deverão ser entregues na Sede do CRM-MG, salvo disposição diversa expressamente indicada na OFB ou em outro documento emitido pela Contratante.

4.15.4. A Contratada deverá fornecer meios para contato e registro de ocorrências relacionadas ao fornecimento, implantação, suporte técnico, manutenção e assistência técnica da solução, contemplando atendimento por meio eletrônico e, quando necessário, por meio telefônico, nos horários e condições definidos neste Termo de Referência, em seus anexos ou no contrato.

4.15.5. O andamento do fornecimento dos equipamentos, licenças, subscrições e demais componentes da solução deverá ser acompanhado pela Contratada, que dará ciência à Contratante de eventuais ocorrências, atrasos, impedimentos, pendências ou fatos que possam impactar o cumprimento dos prazos e condições estabelecidos.

4.15.6. A Contratada deverá manter comunicação clara e tempestiva com a Contratante durante as etapas de fornecimento, entrega, implantação, suporte técnico, manutenção e assistência técnica, prestando as informações necessárias ao acompanhamento e à fiscalização da execução contratual.

4.15.7. As ocorrências registradas, comunicações realizadas, providências adotadas e informações relevantes sobre o fornecimento e acompanhamento da solução deverão ser mantidas pela Contratada e disponibilizadas à Contratante sempre que solicitado.

4.15.8. Eventuais alterações quanto aos itens, quantidades, prazos, locais de entrega ou demais condições constantes da Ordem de Fornecimento de Bens — OFB somente poderão ocorrer mediante autorização formal da Contratante.

4.15.9. A Contratada deverá apresentar, quando aplicável, documentação ou evidências que permitam identificar e rastrear os equipamentos, licenças, subscrições e demais componentes fornecidos, incluindo número de série, modelo, part number, identificador de licença, comprovante de ativação ou informação equivalente.

4.15.10. Qualquer ocorrência que possa comprometer o fornecimento da solução, a entrega, a ativação das licenças ou o cumprimento das condições estabelecidas deverá ser comunicada tempestivamente à Contratante, acompanhada das justificativas e das

providências propostas pela Contratada.

4.16. Requisitos de Segurança da Informação e Privacidade

4.16.1. A Contratada deverá observar as normas de segurança da informação, privacidade, proteção de dados pessoais, confidencialidade, integridade, disponibilidade e rastreabilidade aplicáveis à execução contratual, bem como as orientações e procedimentos internos definidos pelo CRM-MG.

4.16.2. O acesso da Contratada ao ambiente tecnológico do CRM-MG deverá ser previamente autorizado pela Contratante, limitado ao estritamente necessário para a execução do objeto e concedido pelo menor tempo possível, observando-se o princípio do menor privilégio.

4.16.3. Os acessos concedidos aos profissionais da Contratada deverão ser, sempre que tecnicamente possível, identificados, individualizados e rastreáveis, sendo vedado o uso de credenciais genéricas, compartilhadas ou não autorizadas.

4.16.4. A Contratada deverá zelar pela proteção das informações, documentos, dados, configurações, registros, credenciais, diagramas, políticas de segurança, logs, parâmetros técnicos e demais elementos aos quais tiver acesso em razão da execução contratual.

4.16.5. É vedada à Contratada a reprodução, cópia, transferência, divulgação, compartilhamento, retenção ou utilização de informações institucionais do CRM-MG para finalidade diversa da execução contratual, salvo mediante autorização expressa da Contratante.

4.16.6. Os profissionais da Contratada que atuarem na execução do objeto deverão observar dever de sigilo e confidencialidade sobre todas as informações institucionais, técnicas, operacionais e estratégicas a que tiverem acesso, inclusive após o encerramento da relação contratual.

4.16.7. Quando houver necessidade de acesso remoto ao ambiente tecnológico do CRM-MG, este deverá ser previamente autorizado pela Contratante, realizado por meio definido ou aprovado pelo CRM-MG e, sempre que possível, acompanhado por representante técnico da Contratante.

4.16.8. A utilização de ferramentas, softwares, agentes, scripts, mecanismos de coleta, diagnóstico, monitoramento ou acesso remoto pela Contratada deverá ser previamente informada e autorizada pela Contratante, sendo vedada a instalação ou execução de recursos não aprovados no ambiente tecnológico do CRM-MG.

4.16.9. A Contratada deverá comunicar imediatamente ao CRM-MG qualquer incidente, suspeita de incidente, vulnerabilidade, exposição indevida de informações, acesso não autorizado, perda, alteração, indisponibilidade, vazamento ou uso inadequado de dados, sistemas, credenciais ou componentes da solução.

4.16.10. A Contratada deverá colaborar com a Contratante na apuração de incidentes, eventos de segurança, falhas, acessos indevidos ou ocorrências relacionadas à execução contratual, fornecendo informações, registros, evidências e esclarecimentos necessários, quando solicitado.

4.16.11. A Contratada deverá adotar medidas técnicas, administrativas e operacionais adequadas para evitar acesso indevido, uso não autorizado, perda, alteração, divulgação ou tratamento inadequado de informações institucionais ou dados pessoais eventualmente acessados durante a execução contratual.

4.16.12. A Contratada deverá limitar o tratamento de dados e informações ao mínimo necessário para a execução do objeto, observadas as finalidades da contratação e as orientações da Contratante.

4.16.13. A Contratada não poderá manter credenciais, cópias de configurações, bases de dados, documentos técnicos, registros, logs ou quaisquer informações institucionais do CRM-MG após o encerramento das atividades ou do contrato, salvo quando expressamente

autorizado pela Contratante.

4.16.14. Ao final das atividades que exigirem acesso ao ambiente tecnológico, ou sempre que solicitado pela Contratante, os acessos concedidos à Contratada deverão ser revogados, devolvidos, desabilitados ou ajustados, conforme o caso.

4.16.15. As credenciais eventualmente fornecidas à Contratada deverão ser utilizadas exclusivamente para as finalidades autorizadas, sendo vedado o compartilhamento entre profissionais, a reutilização indevida, o armazenamento inseguro ou qualquer uso incompatível com a execução contratual.

4.16.16. A Contratada deverá assegurar que suas atividades, ferramentas, procedimentos e profissionais não comprometam a segurança, a privacidade, a disponibilidade, a integridade ou a confidencialidade do ambiente tecnológico do CRM-MG.

4.16.17. A execução contratual deverá observar a Lei nº 13.709, de 14 de agosto de 2018 — Lei Geral de Proteção de Dados Pessoais, a Lei nº 12.527, de 18 de novembro de 2011 — Lei de Acesso à Informação, as normas internas do CRM-MG e demais disposições legais e regulamentares aplicáveis.

4.17. Outros Requisitos Aplicáveis

4.17.1. A solução deverá ser fornecida de forma completa, integrada, funcional, licenciada, atualizada e apta à utilização no ambiente tecnológico do CRM-MG, observadas as especificações técnicas, quantidades, prazos, condições de entrega, implantação, suporte, garantia e demais requisitos estabelecidos neste Termo de Referência e em seus anexos.

4.17.2. Todos os equipamentos, licenças, subscrições, acessórios, documentações, atualizações, garantias e demais componentes necessários ao funcionamento da solução deverão estar incluídos na proposta da Contratada, não sendo admitida cobrança adicional por itens indispensáveis ao atendimento dos requisitos contratados.

4.17.3. Não será admitido o fornecimento de equipamentos, softwares, licenças, subscrições, garantias ou serviços de suporte em condição irregular, sem origem comprovada, sem cobertura oficial do fabricante, com restrição indevida de uso, sem direito a atualizações, de diferentes fabricantes ou incompatíveis com as condições exigidas neste Termo de Referência.

4.17.4. A Contratada deverá garantir a compatibilidade entre os componentes fornecidos e a solução ofertada, responsabilizando-se por eventuais ajustes, substituições, correções ou providências necessárias para assegurar o pleno funcionamento integrado do objeto contratado.

4.17.5. A solução deverá ser entregue sem restrições indevidas de uso, bloqueios, limitações de licenciamento, dependências não informadas ou condicionantes externas que impeçam sua utilização pelo CRM-MG nos termos previstos neste Termo de Referência.

4.17.6. Quando houver necessidade de registro, ativação, associação ou vinculação de equipamentos, licenças, subscrições, garantias ou suporte técnico junto ao fabricante, tais providências deverão ser realizadas pela Contratada, com comprovação à Contratante, conforme condições estabelecidas neste Termo de Referência.

4.17.7. As licenças, subscrições, garantias e direitos de uso vinculados à solução deverão ser disponibilizados em favor do CRM-MG, pelo período contratado, quando aplicável, sem prejuízo das condições comerciais e técnicas próprias de cada fabricante.

4.17.8. A Contratada deverá assegurar que a solução fornecida esteja apta à utilização regular pelo CRM-MG, inclusive quanto à autenticidade, legalidade, licenciamento, suporte, atualização, garantia e demais condições necessárias ao funcionamento do objeto.

4.17.9. Os requisitos técnicos específicos de cada item, bem como as funcionalidades mínimas exigidas, serão detalhados no Anexo de Especificações Técnicas, prevalecendo a necessidade de atendimento integral ao conjunto da solução.

4.18. Sustentabilidade

4.18.1. Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, deverão ser atendidos, no que couber, os seguintes requisitos, com base no Guia Nacional de Contratações Sustentáveis:

4.18.1.1. A presente contratação deverá observar os princípios da sustentabilidade ambiental previstos na Lei nº 14.133/2021, promovendo, sempre que possível, a redução de impactos ambientais, o uso racional de recursos naturais, a eficiência no consumo de energia e a redução da geração de resíduos.

4.18.1.2. Os equipamentos deverão observar, quando aplicável, critérios de eficiência energética reconhecidos por normas nacionais ou internacionais, incluindo certificação ou etiquetagem emitida pelo INMETRO, no âmbito do Programa Brasileiro de Etiquetagem — PBE, ou por organismo equivalente reconhecido, sem prejuízo do atendimento às especificações técnicas exigidas neste Termo de Referência e em seus anexos.

4.18.1.3. Deverão ser observadas, quando cabíveis, as disposições da Política Nacional de Resíduos Sólidos — Lei nº 12.305/2010, do Decreto nº 10.240/2020 e demais normas aplicáveis, assegurando a destinação ambientalmente adequada de resíduos eletroeletrônicos, componentes, peças, embalagens e demais materiais decorrentes do fornecimento, substituição, manutenção ou assistência técnica dos itens contratados.

4.18.1.4. As embalagens utilizadas deverão, sempre que possível, ser recicláveis, reutilizáveis ou produzidas com materiais de menor impacto ambiental, devendo o material de acondicionamento ser minimizado, observados os princípios da economicidade, da segurança no transporte e da adequada proteção dos equipamentos.

4.18.1.5. Sempre que tecnicamente aplicável, deverão ser priorizados equipamentos fabricados com materiais recicláveis e livres de substâncias perigosas ou restritas, tais como chumbo, cádmio e mercúrio, observadas as diretrizes da Diretiva RoHS — Restriction of Hazardous Substances — ou normas equivalentes.

4.18.1.6. A Contratada deverá adotar boas práticas de responsabilidade socioambiental na execução contratual, observando as normas vigentes de segurança e saúde ocupacional, bem como as obrigações legais aplicáveis de natureza trabalhista, ambiental e previdenciária.

4.18.1.7. A Contratada deverá apresentar, quando solicitado pela Contratante e quando aplicável ao item fornecido, documentação, declaração do fabricante, certificação, manual técnico ou informação equivalente que demonstre o atendimento aos requisitos de sustentabilidade previstos neste Termo de Referência.

4.18.2. O atendimento aos requisitos de sustentabilidade não poderá comprometer a segurança, o desempenho, a compatibilidade, a garantia, o suporte técnico, a disponibilidade ou a funcionalidade da solução contratada.

4.19. Indicação de marcas ou modelos

4.19.1. Não há indicação de marca ou modelo específico para os itens que compõem a solução, sendo admitida a oferta de quaisquer equipamentos, softwares, licenças, subscrições e demais componentes desde que sejam do mesmo fabricante e que atendam integralmente às especificações técnicas, requisitos de desempenho, funcionalidades, condições de suporte, garantia e demais exigências estabelecidas neste Termo de Referência e em seus anexos.

4.19.2. Considerando que o objeto consiste em Solução Integrada de Segurança da Informação, os componentes ofertados deverão compor uma mesma arquitetura tecnológica, com operação integrada, gerenciamento centralizado, aplicação uniforme de políticas, correlação de eventos, rastreabilidade, suporte técnico compatível e funcionamento coordenado entre os elementos da solução.

4.19.3. Para assegurar a integração nativa, a interoperabilidade operacional, a gestão

centralizada, a padronização tecnológica, a responsabilização técnica e a adequada execução do suporte e da garantia, os equipamentos, softwares e subscrições que compõem a solução deverão pertencer ao mesmo fabricante, conforme especificações técnicas deste Termo de Referência e de seus anexos.

4.19.4. A exigência de solução integrada não constitui indicação de marca, fabricante ou modelo específico, mas requisito técnico necessário ao atendimento da necessidade da contratação, especialmente quanto à segurança da informação, gestão centralizada, compatibilidade, continuidade operacional, suporte técnico, atualização, garantia e resposta coordenada a incidentes.

4.19.5. Eventuais referências a padrões tecnológicos, funcionalidades, nomenclaturas, arquiteturas ou características técnicas deverão ser interpretadas como requisitos mínimos ou parâmetros de desempenho, e não como direcionamento a marca ou modelo específico.

4.20. Vedação de marcas ou produtos

4.20.1. Não há vedação prévia à participação de marcas, fabricantes, modelos, produtos ou tecnologias específicas, desde que a solução ofertada atenda integralmente às especificações técnicas, requisitos de desempenho, funcionalidades, condições de integração, suporte, garantia, licenciamento, atualização e demais exigências estabelecidas neste Termo de Referência e em seus anexos.

4.20.2. Não serão aceitos equipamentos, softwares, licenças, subscrições ou componentes que, embora individualmente funcionais, não componham solução integrada de segurança da informação, com operação coordenada, gerenciamento centralizado, aplicação uniforme de políticas, rastreabilidade, suporte compatível e funcionamento aderente à finalidade da contratação.

4.20.3. A eventual incompatibilidade entre os componentes ofertados, a ausência de integração oficial, a dependência de adaptações não previstas, a limitação indevida de funcionalidades, a ausência de suporte compatível ou a impossibilidade de gerenciamento centralizado poderão ensejar a não aceitação da solução, nos termos dos critérios de avaliação técnica previstos neste Termo de Referência.

4.20.4. A vedação de produtos incompatíveis, descontinuados, sem suporte oficial, sem licenciamento regular, sem garantia compatível ou incapazes de compor a solução integrada não constitui restrição indevida à competitividade, mas requisito necessário para assegurar o atendimento da necessidade da contratação, a continuidade operacional, a segurança da informação e a adequada responsabilização técnica da Contratada.

4.21. Exigência de carta de solidariedade

4.21.1. Não será exigida carta de solidariedade emitida pelo fabricante como condição de habilitação ou de apresentação da proposta.

4.21.2. A ausência de exigência de carta de solidariedade não afasta a responsabilidade integral da Contratada pelo fornecimento, implantação, configuração, integração, suporte técnico, garantia, manutenção, atualização, licenciamento e pleno funcionamento da solução durante todo o período contratado.

4.21.3. A Contratada deverá comprovar, no momento definido neste Termo de Referência, no contrato ou quando solicitado pela Contratante, que os equipamentos, softwares, licenças, subscrições, garantias, atualizações e serviços de suporte ofertados possuem origem regular, cobertura oficial, licenciamento válido e suporte compatível com o prazo e as condições exigidas para a solução.

4.21.4. Quando o atendimento de garantia, suporte, atualização, licenciamento ou substituição de componentes depender de fabricante, distribuidor, parceiro autorizado ou rede credenciada, caberá à Contratada assegurar a disponibilidade desses recursos, sem prejuízo de sua responsabilidade integral perante o CRM-MG.

4.21.5. A eventual negativa, limitação, restrição, descontinuidade ou ausência de atendimento por parte do fabricante, distribuidor, parceiro autorizado ou rede credenciada não afastará a responsabilidade da Contratada, que deverá adotar as providências necessárias para garantir o cumprimento integral das obrigações assumidas, sem ônus adicional à Contratante.

4.22. Subcontratação

4.22.1. Não será admitida a subcontratação integral do objeto, nem a transferência da responsabilidade pela execução contratual a terceiros.

4.22.2. Será admitida a participação de fabricante, distribuidor ou parceiro autorizado para execução de atividades acessórias, complementares ou necessárias ao fornecimento, implantação, configuração, suporte técnico, garantia, manutenção, atualização, licenciamento, assistência técnica ou substituição de componentes da solução, desde que preservada a responsabilidade integral da Contratada perante o CRM-MG.

4.22.3. A eventual atuação de terceiros vinculados à Contratada não caracterizará transferência da responsabilidade contratual, cabendo à Contratada coordenar, acompanhar e responder pela qualidade, tempestividade, segurança e conformidade técnica das atividades executadas.

4.22.4. A Contratada deverá assegurar que eventuais terceiros envolvidos na execução de atividades relacionadas ao objeto observem as condições estabelecidas neste Termo de Referência, especialmente quanto à segurança da informação, privacidade, confidencialidade, acesso ao ambiente tecnológico, suporte técnico, garantia, manutenção, assistência técnica e proteção das informações institucionais do CRM-MG.

4.22.5. A Contratada deverá informar previamente à Contratante, quando solicitado ou quando necessário à adequada fiscalização contratual, a participação de terceiros na execução de atividades relacionadas ao objeto, indicando a natureza da atuação, os responsáveis envolvidos e as condições de atendimento.

4.22.6. A participação de terceiros em atividades acessórias, complementares ou especializadas não poderá resultar em prejuízo à integração da solução, à continuidade operacional, ao suporte técnico, à garantia, ao licenciamento, à atualização, à segurança da informação ou ao atendimento dos prazos e demais condições estabelecidas neste Termo de Referência e no contrato.

4.23. Amostra

4.23.1. Não será exigida a apresentação de amostra física dos equipamentos, softwares, licenças, subscrições ou demais componentes da solução, considerando a natureza integrada do objeto, a complexidade técnica da solução, os custos e a inviabilidade operacional de disponibilização prévia dos componentes para simples avaliação amostral.

4.23.2. A não exigência de amostra física não afasta a obrigação da licitante de comprovar a aderência da solução ofertada às especificações técnicas, requisitos de desempenho, funcionalidades, integração, suporte, garantia, licenciamento e demais condições estabelecidas neste Termo de Referência e em seus anexos.

4.23.3. A comprovação da conformidade técnica da solução ofertada deverá ocorrer por meio da proposta, catálogos, datasheets, manuais, folders técnicos, documentação oficial do fabricante, declarações técnicas, páginas oficiais do fabricante ou outros documentos equivalentes aptos a demonstrar o atendimento aos requisitos exigidos, conforme critérios de aceitabilidade da proposta previstos neste Termo de Referência.

4.23.4. A Contratante poderá solicitar esclarecimentos, documentação complementar ou demonstração técnica, quando necessário ao saneamento de dúvidas sobre a aderência da solução ofertada, vedada a criação de exigências novas não previstas neste Termo de Referência.

4.24. Garantia da contratação

4.24.1. Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, com validade durante a execução do contrato e 90 (noventa) dias após término da vigência contratual, 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.

4.24.2. Em caso de opção pelo seguro-garantia, será assegurado à parte adjudicatária prazo mínimo de 1 (um) mês, contado da data de homologação da licitação e anterior à assinatura do contrato, para apresentação da respectiva apólice.

4.24.3. A apólice de seguro-garantia permanecerá em vigor mesmo que o Contratado não pague o prêmio nas datas convencionadas.

4.24.4. Caso o adjudicatário opte pela modalidade seguro-garantia e não apresente a respectiva apólice no prazo estabelecido no edital e antes da assinatura do contrato, ocorrerá a preclusão do direito de escolha dessa modalidade de garantia.

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

4.24.6. 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, ressalvados os períodos de suspensão contratual.

4.24.7. Caso o adjudicatário não opte pelo seguro-garantia ou não apresente a apólice de seguro-garantia antes da assinatura do contrato, deverá apresentar, 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 nas modalidades de caução em dinheiro ou títulos da dívida pública, fiança bancária ou título de capitalização.

4.24.8. Caso seja a garantia em dinheiro a modalidade de garantia escolhida pelo Contratado, deverá ser efetuada em favor do Contratante, em conta específica na Caixa Econômica Federal, com correção monetária.

4.24.9. 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 competente.

4.24.10. 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.

4.24.11. Na hipótese de opção pelo título de capitalização, a garantia deverá ser custeada por pagamento único, com resgate pelo valor total, sob a modalidade de instrumento de garantia, emitido por sociedades de capitalização regularmente constituídas e autorizadas pelo Governo Federal.

4.24.12. O título de capitalização deverá ser apresentado ao Contratante juntamente com as condições gerais e o número do processo administrativo sob o qual o plano de capitalização foi aprovado pela Susep (art. 8º, III, da Circular SUSEP nº 656, de 11 de março de 2022).

4.24.13. A garantia assegurará, qualquer que seja a modalidade escolhida, sob pena de não aceitação, o pagamento de:

4.24.13.1. prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

4.24.13.2. multas moratórias e punitivas aplicadas pela Administração à contratada; e

4.24.13.3. obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pelo Contratado.

4.24.14. Em caso de seguro-garantia, a apólice deverá ter cobertura para pagamento direto ao empregado após decisão definitiva em processo administrativo que apure montante líquido e certo a ele devido em razão de inadimplência do Contratado, independentemente de trânsito em julgado de decisão judicial.

4.24.15. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada ou renovada, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, contado da data de assinatura do termo aditivo ou da emissão do apostilamento, seguindo os mesmos parâmetros utilizados quando da contratação.

4.24.16. 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.

4.24.17. 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, prorrogáveis por igual período, a critério do Contratante, contados da data em que for notificada.

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

4.24.18.1. 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.

4.24.18.2. 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 nº 662, de 11 de abril de 2022.

4.24.19. Extinguir-se-á a garantia com a restituição da carta fiança, autorização para a liberação de importâncias depositadas em dinheiro a título de garantia ou anuência ao resgate do título de capitalização, acompanhada de declaração do Contratante, mediante termo circunstanciado, de que o Contratado cumpriu todas as cláusulas do contrato.

4.24.19.1. A extinção da garantia na modalidade seguro-garantia observará a regulamentação da Susep.

4.24.19.2. A Administração deverá apurar se há alguma pendência contratual antes do término da vigência da apólice.

4.24.20. 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.

4.24.21. O Contratado autoriza o Contratante a reter, a qualquer tempo, a garantia, na forma prevista neste Termo de Referência.

4.24.22. 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.

4.24.23. A garantia de execução é independente de eventual garantia do produto ou serviço prevista neste Termo de Referência.

4.25. **Informações relevantes para o dimensionamento da proposta**

4.25.1. A licitante deverá considerar, para fins de elaboração de sua proposta, todos os requisitos, especificações técnicas, quantitativos, prazos, condições de entrega,

implantação, suporte, garantia, licenciamento, atualizações, treinamento e demais obrigações previstas neste Termo de Referência e em seus anexos.

4.25.2. A proposta deverá contemplar os quantitativos totais previstos neste Termo de Referência e em seus anexos, inclusive quanto à quantidade de equipamentos, endpoints protegidos, licenças, subscrições, garantias, suporte técnico, atualizações, treinamento, instalação, configuração e demais serviços necessários à entrega da solução completa.

4.25.3. A solução deverá atender à Sede do CRM-MG e às Delegacias Regionais contempladas na contratação, observadas as quantidades, características e distribuição lógica dos equipamentos, licenças, subscrições e serviços definidos neste Termo de Referência e no Anexo de Especificações Técnicas.

4.25.4. Independentemente da destinação final dos equipamentos e componentes no ambiente do CRM-MG, os equipamentos, licenças, subscrições e demais componentes da solução deverão ser entregues, como regra, na Sede do CRM-MG, salvo disposição diversa expressamente indicada pela Contratante na Ordem de Fornecimento de Bens — OFB ou em outro documento formal.

4.25.5. A licitante deverá considerar que a instalação física dos equipamentos destinados às Delegacias Regionais será realizada pela equipe interna do CRM-MG, sem prejuízo da responsabilidade da Contratada pela adequada configuração, integração, ativação, suporte à validação técnica e funcionamento dos componentes da solução, conforme condições previstas neste Termo de Referência.

4.25.6. A proposta deverá contemplar todos os equipamentos, softwares, licenças, subscrições, acessórios, cabos, fontes, módulos, garantias, atualizações, suportes, serviços técnicos, documentação e demais componentes necessários ao pleno funcionamento da solução integrada, não sendo admitida cobrança adicional por itens indispensáveis ao atendimento dos requisitos contratados.

4.25.7. A licitante deverá considerar a necessidade de compatibilidade da solução ofertada com o ambiente tecnológico existente do CRM-MG, não sendo admitida a imposição posterior de substituições, aquisições adicionais, adaptações estruturais ou componentes não previstos neste Termo de Referência como condição para o funcionamento da solução.

4.25.8. A licitante deverá considerar as condições existentes de conectividade, infraestrutura lógica e disponibilidade elétrica dos ambientes abrangidos pela contratação, observadas as informações disponibilizadas pela Contratante, não sendo admitida a exigência posterior de adequações não previstas como condição para funcionamento da solução, salvo situações justificadas e formalmente aprovadas pela Contratante.

4.25.9. A licitante deverá considerar que o licenciamento, as subscrições, as atualizações, o suporte técnico, a garantia, a manutenção e a assistência técnica deverão possuir cobertura pelo período de 60 (sessenta) meses, contado da emissão do Termo de Recebimento Definitivo da solução, conforme condições estabelecidas neste Termo de Referência.

4.25.10. No caso de licenças, subscrições ou serviços com cobertura plurianual, especialmente aqueles vinculados à solução de detecção e resposta de endpoint — XDR, a proposta deverá considerar a disponibilização da cobertura contratada pelo período integral de 60 (sessenta) meses, com comprovação de ativação ou disponibilização junto ao fabricante, quando aplicável.

4.25.11. A licitante deverá considerar em sua proposta todos os custos necessários à ativação, manutenção e atualização das funcionalidades contratadas pelo período de 60 (sessenta) meses, incluindo assinaturas, bases de inteligência, atualizações de segurança, firmwares, softwares, subscrições e demais recursos indispensáveis ao funcionamento da solução.

4.25.12. A licitante deverá considerar que a solução pretendida possui natureza integrada, devendo os componentes ofertados compor uma mesma arquitetura tecnológica, com operação integrada, gerenciamento centralizado, aplicação uniforme de políticas,

correlação de eventos, rastreabilidade, suporte técnico compatível e funcionamento coordenado entre os elementos da solução.

4.25.13. A proposta deverá ser acompanhada, quando exigido neste Termo de Referência, no edital ou em seus anexos, de documentação técnica suficiente para demonstrar a aderência da solução ofertada aos requisitos exigidos, tais como catálogos, datasheets, manuais, folders técnicos, documentação oficial do fabricante, declarações técnicas, páginas oficiais do fabricante, comprovação de licenciamento, informações sobre suporte, garantia, atualizações ou documentos equivalentes.

4.25.14. A licitante deverá considerar todos os custos diretos e indiretos necessários à execução integral do objeto, incluindo tributos, fretes, seguros, embalagens, logística, licenciamento, ativação, suporte, garantia, manutenção, assistência técnica, treinamento, deslocamentos eventualmente necessários, ferramentas, mão de obra, encargos e demais despesas necessárias ao cumprimento das obrigações contratuais.

4.25.15. A apresentação da proposta implicará ciência e concordância da licitante quanto às condições estabelecidas neste Termo de Referência, não sendo admitida alegação posterior de desconhecimento das características, requisitos, prazos, responsabilidades, quantitativos ou condições necessárias à execução do objeto.

4.26. Reserva de cotas para ME/EPP

4.26.1. Não será adotada reserva de cota para microempresas e empresas de pequeno porte, considerando a natureza integrada do objeto, a necessidade de fornecimento de solução única, compatível, centralizada e funcional, bem como a interdependência técnica entre os equipamentos, softwares, licenças, subscrições, suporte, garantia, atualizações, implantação e demais componentes da contratação.

4.26.2. A divisão do objeto em cotas ou a reserva de parte do fornecimento poderia comprometer a padronização tecnológica, a integração entre os componentes, o gerenciamento centralizado, a aplicação uniforme de políticas, a continuidade operacional, a responsabilização técnica da Contratada e o suporte da solução durante o período contratado.

4.26.3. A não adoção de reserva de cotas não afasta a possibilidade de participação de microempresas e empresas de pequeno porte no certame, desde que atendidas integralmente as condições de habilitação, qualificação, proposta, fornecimento, suporte, garantia, licenciamento e demais requisitos estabelecidos neste Termo de Referência, no edital e em seus anexos.

4.27. Margem de preferência

4.27.1. Não será aplicada margem de preferência na presente contratação, considerando que não foi identificado enquadramento específico aplicável aos itens que compõem a solução, bem como a natureza do mercado de soluções integradas de segurança da informação, composto predominantemente por fabricantes internacionais.

5. PAPÉIS E RESPONSABILIDADES

5.1. São obrigações da CONTRATANTE:

5.1.1. nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

5.1.2. encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;

5.1.3. receber o objeto fornecido pelo Contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

5.1.4. aplicar à contratada as sanções administrativas regulamentares e contratuais

cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

5.1.5. liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

5.1.6. comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

5.1.7. definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte do Contratado, com base em pesquisas de mercado, quando aplicável; e

5.1.8. prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer.

5.2. São obrigações do CONTRATADO:

5.2.1. indicar formalmente preposto apto a representá-la junto à Contratante, que deverá responder pela fiel execução do contrato;

5.2.2. atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

5.2.3. reparar quaisquer danos diretamente causados à Contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução do contrato pela Contratante;

5.2.4. propiciar todos os meios necessários à fiscalização do contrato pela Contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

5.2.5. manter, durante toda a execução do contrato, as mesmas condições da habilitação;

5.2.6. quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

5.2.7. quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;

5.2.8. ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração; e

5.2.9. fazer a transição contratual, com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos do contratante ou da nova empresa que continuará a execução do contrato, quando for o caso.

6. MODELO DE EXECUÇÃO DO CONTRATO

6.1. Rotinas de Execução

6.2. Do Encaminhamento Formal de Demandas

6.2.1. O gestor do contrato emitirá a Ordem de fornecimento de bens (OFB) para a entrega dos bens desejados.

6.2.2. O Contratado deverá fornecer equipamentos com as mesmas configurações e quantidades definidas na OFB.

6.2.3. O recebimento provisório e definitivo dos bens é disciplinado em tópico próprio

deste TR.

6.3. Forma de execução e acompanhamento do contrato

6.4. Condições de Entrega

6.4.1. O prazo de entrega dos equipamentos, licenças, subscrições e demais componentes necessários à solução será de até 90 (noventa) dias corridos, contado do recebimento da Ordem de Fornecimento de Bens — OFB pela Contratada.

6.4.2. Os bens deverão ser entregues na Sede do CRM-MG, salvo disposição diversa expressamente indicada pela Contratante na Ordem de Fornecimento de Bens — OFB ou em outro documento formal.

6.4.3. A entrega deverá ser acompanhada, quando aplicável, de nota fiscal, relação dos itens fornecidos, identificação de modelos, números de série, part numbers, identificadores de licenças, comprovantes de ativação ou disponibilização, documentação técnica, manuais, termos de garantia e demais documentos necessários à conferência e rastreabilidade dos itens entregues.

6.4.4. A Contratada deverá comunicar formalmente à Contratante, com a devida antecedência, qualquer fato que possa comprometer o prazo ou as condições de entrega, indicando as razões, os impactos previstos e as providências adotadas para regularização.

6.4.5. Não serão aceitos itens entregues em desconformidade com as especificações técnicas, quantidades, prazos, condições de licenciamento, garantia, suporte, atualização ou demais requisitos estabelecidos neste Termo de Referência e em seus anexos.

6.4.6. A entrega dos equipamentos, licenças, subscrições e demais componentes não implica, por si só, recebimento definitivo da solução, o qual dependerá da verificação de conformidade e dos demais procedimentos de recebimento previstos neste Termo de Referência.

6.5. Formas de transferência de conhecimento

6.5.1. A transferência do conhecimento deverá ser realizada observando-se o que segue:

6.5.1.1. realização de treinamento oficial do fabricante, destinado a turma de até 2 (dois) participantes indicados pelo CRM-MG, contemplando os produtos fornecidos e os conhecimentos necessários à administração, operação, monitoramento e acompanhamento da solução;

6.5.1.2. disponibilização, quando aplicável, de materiais de apoio, documentação técnica, manuais, orientações operacionais, certificados ou comprovantes de participação, em formato físico ou eletrônico, compatíveis com os produtos e tecnologias fornecidos;

6.5.1.3. prestação de orientações operacionais iniciais pela Contratada à equipe técnica do CRM-MG sobre a solução efetivamente implantada, incluindo principais componentes, acessos administrativos, funcionalidades, registros, procedimentos básicos de operação, abertura de chamados, acompanhamento do suporte técnico e atualização da solução; e

6.5.1.4. realização da transferência de conhecimento em momento compatível com a implantação e entrada em operação da solução, preferencialmente após a configuração inicial dos principais componentes, de modo a favorecer o aproveitamento prático pela equipe técnica do CRM-MG.

6.6. Procedimentos de transição e finalização do contrato

6.6.1. Os procedimentos de transição e finalização do contrato constituem-se das seguintes etapas:

6.6.1.1. disponibilização, pela Contratada, das informações necessárias à continuidade

da operação da solução, incluindo documentação técnica atualizada, relação de equipamentos, licenças, subscrições, garantias, versões, configurações relevantes, políticas aplicadas, registros de suporte, procedimentos básicos de administração e demais informações necessárias ao acompanhamento da solução pela equipe técnica do CRM-MG;

6.6.1.2. apoio técnico à Contratante, quando solicitado, para esclarecimento de dúvidas relacionadas à operação, suporte, garantia, licenciamento, atualização, substituição de componentes, abertura de chamados junto ao fabricante e demais aspectos necessários à continuidade da utilização da solução até o encerramento contratual;

6.6.1.3. revogação, devolução, desabilitação ou ajuste dos acessos eventualmente concedidos à Contratada, seus profissionais, prepostos ou terceiros envolvidos na execução contratual, observadas as orientações da Contratante e os requisitos de segurança da informação e privacidade previstos neste Termo de Referência;

6.6.1.4. devolução, exclusão ou descarte seguro, conforme orientação da Contratante, de documentos, credenciais, cópias de configurações, registros, arquivos, bases de dados ou quaisquer informações institucionais do CRM-MG eventualmente mantidas pela Contratada em razão da execução contratual, ressalvadas as hipóteses de guarda obrigatória previstas em lei ou expressamente autorizadas pela Contratante;

6.6.1.5. apresentação de relatório ou registro final, quando solicitado pela Contratante, contendo a situação da solução ao término do contrato, pendências existentes, chamados em aberto, garantias vigentes, licenças ativas, atualizações aplicadas, substituições realizadas e demais informações relevantes à finalização contratual;

6.6.1.6. transferência, disponibilização ou confirmação, quando aplicável, dos acessos administrativos, registros, titularidade de licenças, subscrições, garantias, contas, portais do fabricante e demais elementos necessários para que o CRM-MG mantenha a gestão e o acompanhamento da solução após o encerramento contratual, observadas as condições comerciais e técnicas próprias de cada fabricante;

6.6.1.7. tratamento ou encaminhamento formal de chamados, pendências técnicas, substituições, garantias, atualizações ou ocorrências em aberto na data de encerramento contratual, de modo a assegurar a continuidade do acompanhamento pela Contratante e evitar prejuízo à operação da solução.

6.7. Quantidade mínima de bens ou serviços para comparação e controle

6.7.1. Cada Ordem de Fornecimento de Bens — OFB conterá a quantidade a ser fornecida, incluindo os itens correspondentes, a localização de entrega e o prazo aplicável, conforme definições deste Termo de Referência.

6.7.2. Para fins de comparação, conferência e controle, a Contratada deverá observar os quantitativos, especificações, unidades de fornecimento, licenças, subscrições, serviços vinculados e demais componentes previstos neste Termo de Referência e em seus anexos.

6.7.3. O fornecimento deverá permitir a verificação individualizada dos bens, licenças, subscrições e demais componentes entregues, inclusive mediante identificação de modelo, número de série, part number, identificador de licença, comprovante de ativação ou documento equivalente, quando aplicável.

6.7.4. A entrega em quantidade inferior, divergente ou em desconformidade com a OFB, com a proposta aceita ou com as especificações deste Termo de Referência poderá ensejar a não aceitação dos itens, sem prejuízo das demais providências administrativas cabíveis.

6.7.5. A entrega parcial somente será admitida quando previamente autorizada pela Contratante e desde que não comprometa a implantação, a integração, o licenciamento, o suporte, a garantia, o funcionamento da solução ou os prazos estabelecidos neste Termo de Referência.

6.8. Mecanismos formais de comunicação

6.8.1. São definidos como mecanismos formais de comunicação entre a Contratante e a Contratada os seguintes:

6.8.1.1. Ordem de Fornecimento de Bens — OFB;

6.8.1.2. Ata de reunião;

6.8.1.3. Ofício;

6.8.1.4. Sistema de abertura e acompanhamento de chamados;

6.8.1.5. E-mails institucionais;

6.8.1.6. Sistema Eletrônico de Informações — SEI, quando aplicável;

6.8.1.7. Portal, sistema ou ferramenta disponibilizada pela Contratada ou pelo fabricante para registro, acompanhamento e tratamento de chamados, suporte técnico, garantia, licenciamento, atualizações ou assistência técnica, quando aplicável;

6.8.1.8. Outros meios formais previamente aceitos pela Contratante, desde que permitam registro, rastreabilidade e comprovação da comunicação realizada.

6.8.2. As comunicações formais deverão permitir a identificação do remetente, destinatário, data, horário, conteúdo, providências solicitadas ou adotadas e demais informações necessárias ao acompanhamento e à fiscalização da execução contratual.

6.8.3. As comunicações realizadas por meios informais, tais como mensagens instantâneas ou contatos telefônicos, poderão ser utilizadas para alinhamentos operacionais, mas deverão ser formalizadas posteriormente por um dos mecanismos previstos neste item sempre que envolverem decisões, aprovações, alterações, solicitações, ocorrências relevantes ou impactos na execução contratual.

6.9. **Formas de Pagamento**

6.9.1. Os critérios de medição e pagamento serão tratados em tópico próprio do Modelo de Gestão do Contrato.

6.10. **Manutenção de Sigilo e Normas de Segurança**

6.10.1. O Contratado deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução do contrato, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

6.10.2. O Termo de Compromisso e Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal do Contratado, e Termo de Ciência, a ser assinado por todos os empregados do Contratado diretamente envolvidos na contratação, encontram-se nos ANEXOS II e III.

7. **MODELO DE GESTÃO DO CONTRATO**

7.1. 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.

7.2. 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.

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

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

7.5. Reunião Inicial

7.5.1. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada a Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução do contrato.

7.5.2. A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD/ME nº 94, de 2022, e ocorrerá em até 10 dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da Contratante.

7.5.3. A pauta desta reunião observará, pelo menos:

7.5.3.1. Presença do representante legal da contratada, que apresentará o seu preposto;

7.5.3.2. Entrega, por parte da Contratada, do Termo de Compromisso e dos Termos de Ciência;

7.5.3.3. Esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

7.5.3.4. A Carta de apresentação do Preposto deverá conter no mínimo o nome completo e CPF do funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor principal junto à Contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

7.5.3.5. Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste termo de referência.

7.6. Fiscalização

7.6.1. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos, nos termos do art. 33 da IN SGD nº 94, de 2022, observando-se, em especial, as rotinas a seguir.

7.7. Fiscalização Técnica

7.7.1. O fiscal técnico do contrato, além de exercer as atribuições previstas no art. 33, II, da IN SGD nº 94, de 2022, 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.

7.7.2. 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.

7.7.3. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção.

7.7.4. O fiscal técnico do contrato informará ao gestor do contrato, 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.

7.7.5. 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.

7.7.6. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à

prorrogação contratual.

7.8. Fiscalização Administrativa

7.8.1. O fiscal administrativo do contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022, verificará a manutenção das condições de habilitação da Contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamentos e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário.

7.8.2. 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.

7.8.3. Além do disposto acima, a fiscalização contratual obedecerá às seguintes rotinas:

7.8.3.1. verificação da regularidade documental da Contratada durante a execução contratual, especialmente quanto à manutenção das condições de habilitação, regularidade fiscal, trabalhista, previdenciária e demais exigências previstas no edital, no contrato e na legislação aplicável;

7.8.3.2. acompanhamento dos empenhos, notas fiscais, pagamentos, eventuais retenções, glosas, reajustes, repactuações, apostilamentos, termos aditivos e demais atos administrativos relacionados à execução contratual;

7.8.3.3. conferência, em conjunto com a fiscalização técnica quando necessário, da compatibilidade entre os documentos fiscais apresentados e os bens, licenças, subscrições, serviços, garantias, suporte técnico, atualizações e demais componentes efetivamente entregues, ativados ou disponibilizados;

7.8.3.4. acompanhamento da vigência contratual, dos prazos de cobertura de garantia, suporte técnico, licenciamento, subscrições, atualizações e assistência técnica, especialmente quanto ao período de 60 (sessenta) meses contado da emissão do Termo de Recebimento Definitivo da solução;

7.8.3.5. verificação da apresentação, renovação, substituição, complementação ou manutenção de garantia contratual, caso exigida no contrato, observadas as condições previstas no edital, no contrato e na legislação aplicável;

7.8.3.6. registro e comunicação ao gestor do contrato de ocorrências administrativas, atrasos, pendências documentais, inconsistências em documentos fiscais, descumprimentos contratuais ou fatos que possam impactar a execução, o pagamento ou a continuidade contratual;

7.8.3.7. instrução dos autos com documentos, manifestações, registros e evidências necessárias ao acompanhamento administrativo da execução contratual, inclusive para subsidiar eventual apuração de responsabilidade, aplicação de sanções, glosas, apostilamentos, termos aditivos ou encerramento contratual.

7.8.4. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade do Contratado, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade da Contratante ou de seus agentes, gestores e fiscais, de conformidade.

7.9. Gestor do Contrato

7.9.1. Cabe ao gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022:

7.9.1.1. coordenar 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.

7.9.1.2. acompanhar 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.

7.9.1.3. acompanhar a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotar os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais.

7.9.1.4. emitir 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.

7.9.1.5. tomar 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.

7.9.1.6. 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.

7.9.1.7. 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.

7.9.2. 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 prorrogação contratual.

7.10. Critérios de Aceitação

7.10.1. A avaliação da qualidade dos produtos entregues, licenças, subscrições, serviços vinculados e demais componentes da solução, para fins de aceitação, consistirá na verificação dos critérios relacionados a seguir.

7.10.2. Todos os equipamentos fornecidos deverão ser novos, incluindo peças, módulos, fontes, acessórios e demais componentes, de primeiro uso, sem sinais de utilização anterior, não recondicionados, não remanufaturados, não reformados e em fase de comercialização normal pelos canais oficiais ou autorizados do fabricante, não sendo aceitos produtos descontinuados, em fim de comercialização, em fim de suporte ou em fim de vida útil na data de apresentação da proposta.

7.10.3. Todos os componentes dos equipamentos e respectivas funcionalidades deverão ser compatíveis entre si e com a solução ofertada, sem a utilização de adaptações físicas ou lógicas indevidas, procedimentos não previstos nas especificações técnicas, materiais inadequados ou recursos destinados a adaptar forçadamente produtos ou componentes incompatíveis.

7.10.4. Todos os componentes internos dos equipamentos, quando aplicável, deverão estar instalados de forma organizada, adequada e segura, livres de pressões ocasionadas por outros componentes ou cabos que possam causar desconexões, instabilidade, superaquecimento ou funcionamento inadequado.

7.10.5. O número de série de cada equipamento, quando aplicável, deverá ser obrigatório, único e identificável, afixado em local visível no equipamento e/ou na embalagem, devendo ser reconhecido pelo fabricante como válido para o produto entregue e compatível com as condições de garantia, suporte e assistência técnica aplicáveis ao mercado brasileiro.

7.10.6. Serão recusados os produtos que possuam componentes, peças ou acessórios

com sinais claros de oxidação, danos físicos, sujeira, riscos, avarias, violação, desgaste ou qualquer outro indício incompatível com a condição de produto novo e de primeiro uso.

7.10.7. Os produtos, considerando a marca e o modelo apresentados na proposta, não poderão estar fora de linha comercial na data de abertura da licitação ou apresentação da proposta, conforme o caso. Os produtos deverão ser fornecidos completos e prontos para utilização, acompanhados de todos os acessórios, componentes, cabos, fontes, módulos, documentação e demais itens necessários ao seu adequado funcionamento, conforme especificações deste Termo de Referência e de seus anexos.

7.10.8. As licenças, subscrições, softwares, atualizações, garantias, suporte técnico e demais direitos de uso vinculados à solução deverão estar devidamente regularizados, ativados ou disponibilizados em favor do CRM-MG, pelo período contratado de 60 (sessenta) meses, quando aplicável, não sendo admitidas versões de avaliação, demonstração, "trial", "shareware" ou quaisquer modalidades que limitem indevidamente o uso, a atualização, o suporte ou a continuidade da solução.

7.10.9. A Contratada deverá comprovar, quando aplicável, a ativação, disponibilização ou regularidade das licenças, subscrições, garantias, atualizações e suporte técnico junto ao fabricante, mediante documentação oficial, registro em portal, certificado de licenciamento, termo de ativação, entitlement, identificador de licença ou documento equivalente.

7.10.10. A Contratante poderá avaliar a qualidade e conformidade de todos os equipamentos, licenças, subscrições e demais componentes fornecidos ou, quando cabível, realizar verificação por amostragem, sem prejuízo da exigência de documentação, registros, evidências técnicas, testes de funcionamento e demais elementos necessários à comprovação da aderência da solução aos requisitos estabelecidos neste Termo de Referência.

7.10.11. A Contratante poderá solicitar catálogos, datasheets, manuais, documentação oficial do fabricante, registros de ativação, comprovantes de garantia, informações de suporte, evidências de licenciamento, relatórios de testes ou outros documentos equivalentes para subsidiar a análise de conformidade técnica dos itens entregues.

7.10.12. Os testes de aceitação deverão ser registrados nos autos do processo administrativo, contendo, quando aplicável, identificação dos itens avaliados, números de série, licenças, versões, funcionalidades verificadas, resultados obtidos, pendências identificadas e providências adotadas, para fins de rastreabilidade e fiscalização contratual.

7.10.13. Só haverá recebimento definitivo após a análise da qualidade dos bens, licenças, subscrições, serviços vinculados e demais componentes da solução, em face da aplicação dos critérios de aceitação, resguardando-se à Contratante o direito de não receber o objeto cuja qualidade seja comprovadamente baixa, incompleta, irregular ou em desacordo com as especificações definidas neste Termo de Referência e em seus anexos, situação em que poderão ser aplicadas à Contratada as penalidades previstas em lei, no edital, neste Termo de Referência e no contrato.

7.10.14. Quando for o caso, a Contratada será convocada a corrigir, substituir, complementar, regularizar ou refazer, sem custo adicional para a Contratante, todos os bens, licenças, subscrições, serviços ou componentes rejeitados, sem prejuízo dos prazos, responsabilidades e demais consequências previstas neste Termo de Referência e no contrato.

7.11. Procedimentos de Teste e Inspeção

7.11.1. Serão adotados como procedimentos de teste e inspeção, para fins de elaboração dos Termos de Recebimento Provisório e Definitivo (anexos IV e V):

7.11.1.1. conferência física e documental dos equipamentos, licenças, subscrições e demais componentes entregues, incluindo verificação de quantidades, modelos, números de série, part numbers, identificadores de licença, documentação técnica, termos de garantia, comprovantes de ativação, notas fiscais e demais documentos necessários à rastreabilidade

dos itens fornecidos;

7.11.1.2. verificação da conformidade dos equipamentos, softwares, licenças, subscrições e demais componentes da solução com as especificações técnicas, requisitos de desempenho, funcionalidades mínimas, condições de licenciamento, suporte, garantia, atualização e demais exigências estabelecidas neste Termo de Referência, no edital, na proposta aceita e em seus anexos;

7.11.1.3. realização de testes de instalação, configuração, integração, comunicação, gerenciamento centralizado, aplicação de políticas, atualização, registro de logs e eventos, conectividade, funcionamento dos recursos de proteção e administração da solução, conforme aplicável aos componentes efetivamente fornecidos;

7.11.1.4. validação da ativação ou disponibilização das licenças, subscrições, garantias, atualizações e suporte técnico pelo período contratado, especialmente quanto à cobertura de 60 (sessenta) meses, mediante documentação oficial do fabricante, registro em portal, certificado de licenciamento, termo de ativação, entitlement ou documento equivalente;

7.11.1.5. verificação da integração entre os componentes da solução, incluindo firewalls de próxima geração, equipamento de gerenciamento centralizado, switches, access points e solução de detecção e resposta de endpoint — XDR, de modo a confirmar a operação coordenada, o gerenciamento centralizado, a rastreabilidade e o funcionamento aderente à finalidade da contratação;

7.11.1.6. registro dos testes, inspeções, validações, pendências, inconformidades e providências adotadas em documento próprio, relatório técnico, checklist, termo de verificação ou instrumento equivalente, a ser juntado aos autos do processo administrativo para fins de rastreabilidade e fiscalização contratual.

7.11.1.7. validação, quando aplicável, dos recursos de alta disponibilidade previstos para os componentes críticos da Sede, especialmente quanto aos firewalls de próxima geração destinados ao ambiente central, de modo a verificar a aderência da configuração aos requisitos definidos neste Termo de Referência e em seus anexos;

7.11.1.8. verificação dos acessos administrativos, perfis de usuários, permissões, rastreabilidade de ações e demais parâmetros de administração da solução, conforme definições aprovadas pela Contratante;

7.11.1.9. verificação da atualização inicial dos componentes da solução, incluindo versões de firmware, software, assinaturas, bases de inteligência, correções de segurança e demais recursos necessários ao funcionamento adequado da solução;

7.11.1.10. validação da comunicação dos componentes remotos com o ambiente de gerenciamento centralizado, quando aplicável, especialmente após a ativação dos equipamentos destinados às Delegacias Regionais;

7.11.1.11. verificação dos canais de suporte técnico, garantia e assistência técnica disponibilizados pela Contratada ou pelo fabricante, incluindo, quando aplicável, a possibilidade de abertura, acompanhamento e registro de chamados relacionados à solução.

7.11.2. Eventuais falhas, divergências, pendências ou inconformidades identificadas durante os procedimentos de teste e inspeção deverão ser comunicadas à Contratada para correção, substituição, complementação, regularização ou reapresentação dos itens, sem ônus adicional à Contratante e sem prejuízo das demais providências cabíveis.

7.12. Níveis Mínimos de Serviço Exigidos

7.12.1. Os níveis mínimos de serviço são indicadores mensuráveis estabelecidos pelo Contratante para aferir objetivamente os resultados pretendidos com a contratação. São considerados para a presente contratação os seguintes indicadores:

IAE - INDICADOR DE ATRASO NO FORNECIMENTO	
Tópico	Descrição

IAE - INDICADOR DE ATRASO NO FORNECIMENTO	
Tópico	Descrição
Finalidade	Medir o tempo de atraso na entrega dos equipamentos, licenças, subscrições e demais componentes constantes da Ordem de Fornecimento de Bens — OFB.
Meta a cumprir	$IAE \leq 0$. A meta definida visa garantir a entrega dos equipamentos, licenças, subscrições e demais componentes constantes da OFB dentro do prazo previsto.
Instrumento de medição	Ordem de Fornecimento de Bens — OFB e Termo de Recebimento Provisório — TRP.
Forma de acompanhamento	A avaliação será feita conforme linha de base registrada na OFB. Será considerado o prazo decorrido entre a data de início da execução da OFB e a data de entrega dos itens constantes da OFB, desde que a entrega seja reconhecida pelo fiscal técnico, com registro no Termo de Recebimento Provisório — TRP.
Periodicidade	Para cada Ordem de Fornecimento de Bens encerrada e com respectivo Termo de Recebimento Definitivo.
Mecanismo de cálculo	$IAE = TEX - TEST$.
Definições	IAE: Indicador de Atraso no Fornecimento da OFB. TEX: Tempo de Execução, correspondente ao período de execução da OFB, contado da sua data de início até a data de entrega dos itens constantes da OFB. TEST: Tempo Estimado para execução da OFB, constante da própria OFB, conforme prazo estipulado neste Termo de Referência.
Data de início da OFB	A data de início será aquela expressamente indicada na OFB. Caso não esteja explícita, será considerado o primeiro dia útil após a emissão da OFB.
Data de entrega da OFB	A data de entrega será aquela reconhecida pelo fiscal técnico, conforme os critérios constantes neste Termo de Referência. Nos casos em que o fiscal técnico rejeitar a entrega, o prazo de execução da OFB continuará a correr, encerrando-se somente quando a Contratada entregar os itens em conformidade e houver aceitação pelo fiscal técnico.
Observações	Serão utilizados dias corridos na medição. Os dias com expediente parcial no CRM-MG serão considerados como dias corridos no cômputo do indicador.

IAE - INDICADOR DE ATRASO NO FORNECIMENTO	
Tópico	Descrição
Início de vigência	A partir da emissão da OFB.
Faixas de ajuste no pagamento e sanções	Para valores do indicador IAE: IAE menor ou igual a 0: pagamento integral da OFB; IAE de 1 a 60: aplicação de glosa de 0,1666% por dia de atraso sobre o valor da OFB ou da fração em atraso; IAE acima de 60: aplicação de glosa de 10%, sem prejuízo de multa de 2% sobre o valor da OFB ou da fração em atraso e demais providências cabíveis.

ITS — Indicador de Tempo de Solução de Chamados Técnicos	
Tópico	Descrição
Finalidade	Medir o tempo de solução dos chamados técnicos relacionados à solução contratada durante o período de garantia, suporte técnico, manutenção e assistência técnica.
Meta a cumprir	Solucionar os chamados técnicos dentro dos prazos máximos definidos neste indicador, conforme a criticidade da ocorrência.
Instrumento de medição	Sistema de abertura e acompanhamento de chamados, portal da Contratada, portal do fabricante, e-mails institucionais, relatórios de atendimento ou outro meio formal de comunicação previsto neste Termo de Referência.
Forma de acompanhamento	A avaliação será realizada com base nos registros de abertura, classificação, acompanhamento, solução e encerramento dos chamados técnicos, considerando a data e horário de abertura do chamado pela Contratante e a data e horário de solução reconhecida pela fiscalização técnica.
Periodicidade	Mensal, durante o período de garantia, suporte técnico, manutenção e assistência técnica da solução.
Mecanismo de cálculo	ITS = TSC - TMS.
Definições	ITS: Indicador de Tempo de Solução do Chamado Técnico. TSC: Tempo de Solução do Chamado, correspondente ao período entre a abertura do chamado pela Contratante e a solução reconhecida pela fiscalização técnica. TMS: Tempo Máximo de Solução previsto para a respectiva criticidade.

ITS — Indicador de Tempo de Solução de Chamados Técnicos	
Tópico	Descrição
Classificação de criticidade	Crítica: falha que cause indisponibilidade total de componente essencial da solução ou impacto relevante à segurança, conectividade ou continuidade dos serviços institucionais. Alta: falha que cause degradação relevante, perda parcial de funcionalidade ou impacto significativo na administração, proteção ou monitoramento da solução. Média: falha que afete funcionalidade não crítica, gere instabilidade pontual ou demande correção sem impacto relevante à continuidade dos serviços. Baixa: dúvida, orientação técnica, ajuste operacional, solicitação de informação ou ocorrência sem impacto direto no funcionamento da solução.
Prazos máximos de solução	Crítica: até 2 (dois) dias úteis. Alta: até 5 (cinco) dias úteis. Média: até 10 (dez) dias úteis. Baixa: até 15 (quinze) dias úteis.
Observações	Os prazos serão contados a partir da abertura do chamado pela Contratante, desde que acompanhada das informações mínimas necessárias ao atendimento. Quando a solução depender de atuação do fabricante, distribuidor, parceiro autorizado, rede credenciada, substituição de peças, RMA, atualização oficial ou condição externa à atuação direta da Contratada, esta deverá comprovar o escalonamento tempestivo, manter acompanhamento ativo e prestar informações periódicas à Contratante até a solução definitiva.
Suspensão justificada do prazo	O prazo poderá ser suspenso, mediante registro formal, quando a continuidade do atendimento depender de informação, autorização, acesso, janela de manutenção, validação ou providência a cargo da Contratante, voltando a correr após a eliminação do impedimento.
Encerramento do chamado	O chamado somente será considerado solucionado após validação pela Contratante ou após comprovação objetiva da correção, restauração, substituição, orientação ou providência técnica suficiente para sanar a ocorrência registrada.

ITS — Indicador de Tempo de Solução de Chamados Técnicos	
Tópico	Descrição
Faixas de ajuste no pagamento e sanções	O descumprimento injustificado do indicador ITS acarretará: na primeira ocorrência no período de apuração, advertência; em caso de reincidência no período de apuração, glosa de 1% sobre o valor mensal proporcional da garantia, suporte técnico, manutenção e assistência técnica; em caso de descumprimento reiterado, ausência de acompanhamento do chamado ou impacto relevante à operação da solução, multa de 2% sobre o valor da parcela afetada, sem prejuízo das demais sanções cabíveis.

8. INFRAÇÕES E SANÇÕES ADMINISTRATIVAS E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NOS PAGAMENTOS

8.1. Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pela Contratante, conforme a tabela abaixo:

Id	Ocorrência	Glosa / Sanção
1	Não prestar, no prazo estabelecido pela Contratante, esclarecimentos solicitados sobre a execução do contrato, salvo quando se tratar de questão técnica de maior complexidade, hipótese em que a Contratada deverá justificar a necessidade de prazo adicional e indicar previsão de resposta.	Advertência. Em caso de atraso injustificado, reincidência ou prejuízo ao acompanhamento da execução contratual, poderá ser aplicada multa de 0,5% sobre o valor da OFB, da parcela em execução ou da obrigação afetada, conforme o caso, por ocorrência.
2	Não atender ao indicador de nível de serviço IAE — Indicador de Atraso no Fornecimento.	Aplicar-se-ão as glosas e sanções previstas no próprio indicador IAE, conforme as faixas definidas neste Termo de Referência: IAE menor ou igual a 0: pagamento integral da OFB; IAE de 1 a 60: glosa de 0,1666% por dia de atraso sobre o valor da OFB ou da fração em atraso; IAE acima de 60: glosa de 10%, sem prejuízo de multa de 2% sobre o valor da OFB ou da fração em atraso e demais providências cabíveis.

Id	Ocorrência	Glosa / Sanção
3	Não atender ao indicador de nível de serviço ITS — Indicador de Tempo de Solução de Chamados Técnicos.	Advertência na primeira ocorrência. Em caso de reincidência, poderá ser aplicada glosa de 1% sobre o valor mensal proporcional da garantia, suporte técnico, manutenção e assistência técnica. Em caso de descumprimento reiterado, ausência de acompanhamento do chamado ou impacto relevante à operação da solução, poderá ser aplicada multa de 2% sobre o valor da parcela afetada, sem prejuízo das demais sanções cabíveis.
4	Entregar equipamentos, licenças, subscrições, acessórios, componentes ou demais itens em desconformidade com as especificações técnicas, quantidades, condições de licenciamento, garantia, suporte, atualização, documentação, proposta aceita ou demais requisitos estabelecidos neste Termo de Referência, no edital, em seus anexos ou no contrato.	Recusa total ou parcial do item em desconformidade, com obrigação de correção, substituição, complementação ou regularização pela Contratada, sem ônus adicional à Contratante. Em caso de não regularização no prazo definido pela fiscalização, poderá ser aplicada multa de 2% sobre o valor da parcela afetada, sem prejuízo das demais sanções cabíveis.
5	Não comprovar ou deixar de manter, quando aplicável, a ativação, disponibilização, regularidade ou cobertura das licenças, subscrições, garantias, atualizações ou suporte técnico pelo período contratado.	Suspensão do pagamento da parcela correspondente até a efetiva regularização e comprovação da cobertura contratada. Persistindo a irregularidade no prazo definido pela fiscalização, poderá ser aplicada multa de 5% sobre o valor da parcela afetada, sem prejuízo da recusa do recebimento, da glosa correspondente e das demais sanções cabíveis.

Id	Ocorrência	Glosa / Sanção
6	Não corrigir, substituir, complementar ou regularizar, no prazo estabelecido pela fiscalização, bens, licenças, subscrições, serviços ou componentes rejeitados ou apontados como pendentes.	Advertência, manutenção da recusa ou pendência e concessão de prazo para regularização, quando cabível. Persistindo a irregularidade, ou havendo reincidência ou prejuízo à execução contratual, poderá ser aplicada multa de 1% sobre o valor da parcela afetada, por ocorrência, limitada a 10%, sem prejuízo das demais sanções cabíveis.
7	Descumprir obrigações relativas à segurança da informação, privacidade, sigilo, confidencialidade, controle de acesso, uso de credenciais, proteção de dados ou tratamento de informações institucionais do CRM-MG.	Advertência, quando se tratar de falha formal ou de menor gravidade, sem prejuízo da imediata correção da irregularidade. Em caso de reincidência, descumprimento relevante, exposição indevida de informações, uso inadequado de credenciais, acesso não autorizado, vazamento de dados, comprometimento do ambiente tecnológico ou prejuízo à Contratante, poderá ser aplicada multa de 5% sobre o valor total do contrato, sem prejuízo da apuração de responsabilidade, reparação integral de danos, comunicação às autoridades competentes, quando aplicável, e demais sanções cabíveis.

Id	Ocorrência	Glosa / Sanção
8	Utilizar ferramentas, softwares, agentes, scripts, mecanismos de coleta, diagnóstico, monitoramento ou acesso remoto sem autorização da Contratante, quando exigida.	Advertência e determinação de interrupção imediata da prática, remoção do recurso não autorizado e regularização da ocorrência, quando cabível. Em caso de risco à segurança da informação, acesso indevido, reincidência, dano, indisponibilidade, coleta não autorizada de informações ou descumprimento relevante das orientações da Contratante, poderá ser aplicada multa de 2% sobre o valor total do contrato, sem prejuízo da apuração de responsabilidade, reparação integral de danos e demais sanções cabíveis.
9	Deixar de manter, durante a execução contratual, as condições de habilitação, regularidade fiscal, trabalhista, previdenciária ou demais exigências aplicáveis.	Notificação da Contratada para regularização, observados os prazos legais e contratuais aplicáveis. Persistindo a irregularidade, poderão ser adotadas as providências administrativas cabíveis, inclusive comunicação aos órgãos competentes, retenção ou suspensão de pagamento quando legalmente admitida, impedimento de prorrogação, extinção contratual e aplicação das sanções previstas no edital, no contrato e na legislação aplicável, conforme o caso.
10	Não manter comunicação adequada, não registrar ocorrências, não disponibilizar informações de acompanhamento ou não apresentar documentação/evidências necessárias à fiscalização contratual.	Advertência e solicitação de regularização da comunicação, registro, documentação ou evidência pendente. Em caso de reincidência, atraso injustificado ou prejuízo ao acompanhamento da execução contratual, poderá ser aplicada multa de 0,5% sobre o valor da OFB, da parcela em execução ou da obrigação afetada, conforme o caso, por ocorrência.

Id	Ocorrência	Glosa / Sanção
11	Não cumprir qualquer outra obrigação contratual não citada nesta tabela.	Advertência. Em caso de reincidência, descumprimento injustificado, não regularização no prazo definido pela fiscalização ou configurado prejuízo aos resultados pretendidos com a contratação, poderá ser aplicada multa de 1% sobre o valor da OFB, da parcela em execução ou da obrigação afetada, conforme o caso, sem prejuízo das demais sanções cabíveis.

8.2. Nos termos do art. 19, inciso III, da Instrução Normativa SGD/ME nº 94, de 2022, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, nos casos em que a Contratada:

8.2.1. não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou

8.2.2. deixar de utilizar materiais, equipamentos, licenças, subscrições, componentes ou recursos humanos exigidos para fornecimento da solução de TIC, ou utilizá-los com qualidade ou quantidade inferior à demandada.

8.3. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, a Contratada 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) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

f) praticar ato fraudulento na execução do contrato;

g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

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

8.4. Serão aplicadas à Contratada que incorrer nas infrações acima descritas as seguintes sanções:

8.4.1. Advertência, quando a Contratada der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave;

8.4.2. Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima, sempre que não se justificar a imposição de penalidade mais grave;

8.4.3. Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave;

8.4.4. Multa:

8.4.4.1. Moratória, para a infração descrita no item “d”, correspondente ao retardamento da execução ou da entrega do objeto da contratação sem motivo justificado, observadas as faixas, percentuais e critérios definidos no IAE — Indicador de Atraso no Fornecimento, previsto neste Termo de Referência, sem prejuízo da aplicação das demais sanções cabíveis quando a mora comprometer a execução contratual ou a utilidade da prestação.

8.4.4.2. Compensatória, para as infrações descritas nas alíneas “e” a “h”, de 10% (dez por cento) a 20% (vinte por cento) do valor da contratação, observada a gravidade da conduta, a extensão do dano causado, a vantagem auferida ou pretendida pela Contratada, a reincidência, as circunstâncias do caso concreto e o devido processo administrativo.

8.4.4.3. Compensatória, para a inexecução total do contrato prevista na alínea “c”, de 10% (dez por cento) a 15% (quinze por cento) do valor da contratação, observada a gravidade da conduta, a extensão do prejuízo causado à Contratante, a fase de execução contratual, a eventual entrega parcial aproveitável, a reincidência, as circunstâncias do caso concreto e o devido processo administrativo.

8.4.4.4. Compensatória, para a infração descrita na alínea “b”, correspondente à inexecução parcial do contrato, de até 10% (dez por cento) sobre o valor da OFB, da parcela em execução, da obrigação inadimplida ou da parcela afetada, conforme o caso, observada a gravidade da conduta, a extensão do prejuízo causado à Contratante, a utilidade da parcela eventualmente executada, a reincidência, as circunstâncias do caso concreto e o devido processo administrativo.

8.4.4.5. Compensatória, em substituição à multa moratória para a infração descrita na alínea “d”, de até 10% (dez por cento) sobre o valor da OFB, da parcela em atraso, da obrigação afetada ou da contratação, conforme o caso, quando o atraso injustificado comprometer a utilidade da prestação, inviabilizar a execução da Ordem de Fornecimento de Bens, caracterizar recusa injustificada de execução, ensejar a extinção contratual ou causar prejuízo relevante à Contratante, observada a gravidade da conduta, a extensão do dano, a fase da execução contratual, a reincidência, as circunstâncias do caso concreto e o devido processo administrativo.

8.4.4.6. Compensatória, para a infração descrita na alínea “a”, correspondente à inexecução parcial do contrato, de até 5% (cinco por cento) sobre o valor da OFB, da parcela em execução, da obrigação inadimplida ou da parcela afetada, conforme o caso, observada a gravidade da conduta, a extensão do prejuízo causado à Contratante, a utilidade da parcela eventualmente executada, a possibilidade de regularização, a reincidência, as circunstâncias do caso concreto e o devido processo administrativo.

8.5. A aplicação das sanções previstas neste Termo de Referência não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante.

8.6. Todas as sanções previstas neste Termo de Referência poderão ser aplicadas cumulativamente com a multa.

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

8.8. 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 descontada da garantia prestada ou será cobrada judicialmente.

8.9. A multa poderá ser recolhida administrativamente no prazo máximo de 15 (quinze) dias úteis, a contar da data do recebimento da comunicação enviada pela autoridade competente.

8.10. 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.

8.10.1. Para a garantia da ampla defesa e contraditório, as notificações serão enviadas eletronicamente para os endereços de e-mail informados na proposta comercial, bem como

os cadastrados pela empresa no SICAF.

8.10.2. Os endereços de e-mail informados na proposta comercial e/ou cadastrados no SICAF serão considerados de uso contínuo da empresa, não cabendo alegação de desconhecimento das comunicações a eles comprovadamente enviadas.

8.11. Na aplicação das sanções serão considerados:

8.11.1. a natureza e a gravidade da infração cometida;

8.11.2. as peculiaridades do caso concreto;

8.11.3. as circunstâncias agravantes ou atenuantes;

8.11.4. os danos que dela provierem para o Contratante; e

8.11.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

8.12. 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.

8.13. 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 Termo de Referência 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.

8.14. O Contratante deverá, no prazo máximo de 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.

8.14.1. As penalidades serão obrigatoriamente registradas no SICAF.

8.15. 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, de 2021.

8.16. 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.

9. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

9.1. Recebimento do Objeto

9.1.1. Os bens serão recebidos provisoriamente, de forma sumária, no ato da entrega, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.

9.1.2. Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 10 (dez) dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

9.1.3. O recebimento definitivo ocorrerá no prazo de 10 (dez) dias úteis, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado.

9.1.4. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

9.1.5. 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 quanto à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

9.1.6. O prazo para a solução, pelo Contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

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

9.1.8. As atividades de montagem, instalação e quaisquer outras necessárias para o funcionamento ou uso do bem correrão por conta do Contratado e são condição para o recebimento do objeto.

9.2. Liquidação

9.2.1. 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, §3º da Instrução Normativa SEGES/ME nº 77/2022.

9.2.2. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso 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.

9.2.3. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

- 9.2.3.1. o prazo de validade;
- 9.2.3.2. a data da emissão;
- 9.2.3.3. os dados do contrato e do órgão contratante;
- 9.2.3.4. o período respectivo de execução do contrato;
- 9.2.3.5. o valor a pagar; e
- 9.2.3.6. eventual destaque do valor de retenções tributárias cabíveis.

9.2.4. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, 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 ao Contratante;

9.2.5. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado 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, de 2021.

9.2.6. A Administração deverá realizar consulta ao SICAF para:

- 9.2.6.1. verificar a manutenção das condições de habilitação exigidas;
- 9.2.6.2. identificar possível razão que impeça a participação em licitação/contratação no âmbito do órgão ou entidade, tais como a proibição de contratar com a Administração ou com o Poder Público, bem como ocorrências impeditivas indiretas.
- 9.2.7. 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.
- 9.2.8. 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.
- 9.2.9. 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.
- 9.2.10. 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.

9.3. **Prazo de pagamento**

- 9.3.1. O pagamento será efetuado no prazo 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.
- 9.3.2. No caso de atraso pela Contratante, os valores devidos à Contratada serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do Índice Nacional de Preços ao Consumidor — INPC/IBGE.

9.4. **Forma de pagamento**

- 9.4.1. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo Contratado.
- 9.4.2. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.
- 9.4.3. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.
- 9.4.4. 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.
- 9.4.5. 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.

9.5. **Antecipação de pagamento**

- 9.5.1. Será admitido, excepcionalmente, o pagamento antecipado correspondente ao item 9, nos termos do art. 145, § 1º, da Lei nº 14.133/2021, considerando as características técnicas e comerciais da solução, na qual o licenciamento, as atualizações, o suporte

técnico oficial do fabricante e a garantia são disponibilizados mediante aquisição, ativação e registro da cobertura integral pelo período de 60 (sessenta) meses.

9.5.2. O pagamento integral do item 9 somente será efetuado após a comprovação da ativação, disponibilização e registro, junto ao fabricante, do licenciamento, das atualizações, do suporte técnico e da garantia pelo período integral de 60 (sessenta) meses, bem como após o respectivo recebimento pela Contratante.

9.5.3. Na hipótese de inexecução total ou parcial das obrigações abrangidas pelo pagamento antecipado, a Contratada deverá devolver à Contratante o valor correspondente à parcela não executada, nos termos do art. 145, § 3º, da Lei nº 14.133/2021, sem prejuízo das demais medidas e sanções cabíveis.

9.6. Cessão de Crédito

9.6.1. As cessões de crédito dependerão de prévia aprovação do Contratante.

9.6.1.1. A eficácia da cessão de crédito, em relação à Administração, está condicionada à celebração de termo aditivo ao contrato administrativo.

9.6.1.2. Sem prejuízo do regular atendimento da obrigação contratual de cumprimento de todas as condições de habilitação por parte do Contratado (cedente), a celebração do aditamento de cessão de crédito e a realização dos pagamentos respectivos também se condicionam à regularidade fiscal e trabalhista do cessionário, bem como à certificação de que o cessionário não se encontra impedido de licitar e contratar com o Poder Público, conforme a legislação em vigor, ou de receber benefícios ou incentivos fiscais ou creditícios, direta ou indiretamente, conforme o art. 12 da Lei nº 8.429, de 1992, nos termos do Parecer JL-01, de 18 de maio de 2020.

9.6.1.3. O crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (Contratado) pela execução do objeto contratual, restando absolutamente incólumes todas as defesas e exceções ao pagamento e todas as demais cláusulas exorbitantes ao direito comum aplicáveis no regime jurídico de direito público incidente sobre os contratos administrativos, incluindo a possibilidade de pagamento em conta vinculada ou de pagamento pela efetiva comprovação do fato gerador, quando for o caso, e o desconto de multas, glosas e prejuízos causados à Administração.

9.6.1.4. A cessão de crédito não afetará a execução do objeto contratado, que continuará sob a integral responsabilidade do Contratado.

9.6.2. O disposto nesta seção não afeta as operações de crédito de que trata a Instrução Normativa SEGES/MGI nº 82, de 21 de fevereiro de 2025, as quais ficam por esta regidas.

9.7. Reajuste

9.7.1. Os preços inicialmente contratados são fixos e irrealizáveis no prazo de um ano contado da data do orçamento estimado, em 14/07/2026.

9.7.2. Após o interregno de um ano, e independentemente de pedido do contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

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

9.7.4. 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).

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

9.7.6. 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.

9.7.7. 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.

9.7.8. O reajuste será realizado por apostilamento.

10. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E FORMA DE FORNECIMENTO

10.1. Forma de seleção e critério de julgamento da proposta

10.1.1. 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 menor preço global.

10.2. Forma de fornecimento

10.2.1. O fornecimento do objeto será integral, compreendendo a entrega dos bens, licenças, subscrições e demais componentes da solução, bem como a execução dos serviços de instalação, configuração, ativação e transferência de conhecimento, sem prejuízo das obrigações de garantia, suporte técnico, atualizações, assistência técnica e manutenção da regularidade das licenças e subscrições pelo período contratado.

10.3. Critérios de aceitabilidade de preços

10.3.1. O critério de aceitabilidade será o menor preço global, observados o valor global estimado da contratação e os valores unitários máximos constantes da planilha de composição de preços anexa ao edital ou da tabela constante deste Termo de Referência.

10.3.2. Serão desclassificadas as propostas que apresentarem preço global superior ao valor máximo aceitável definido pela Administração, bem como aquelas que apresentarem preços unitários manifestamente inexequíveis, incompatíveis com os preços de mercado ou superiores aos limites unitários estabelecidos, quando aplicável.

10.4. Exigências de habilitação

10.4.1. Para fins de habilitação, deverá o interessado comprovar os seguintes requisitos:

10.4.2. Habilitação jurídica

10.4.2.1. 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;

10.4.2.2. empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

10.4.2.3. 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>;

10.4.2.4. 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;

10.4.2.5. 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;

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

10.4.2.7. 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;

10.4.2.8. 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.

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

10.4.3. Habilitação fiscal, social e trabalhista

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

10.4.3.2. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas 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;

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

10.4.3.4. 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;

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

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

10.4.3.7. Caso o fornecedor seja considerado isento dos tributos 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.

10.4.3.8. 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.

10.4.4. Qualificação Econômico-Financeira

10.4.4.1. Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do interessado, caso se trate de pessoa física, desde que admitida a sua participação na licitação/contratação, ou de sociedade simples;

10.4.4.2. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor;

10.4.4.3. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, já exigíveis e apresentados na forma da lei, comprovando índices de Liquidez Geral (LG), Liquidez Corrente (LC) e Solvência Geral (SG) superiores a 1 (um), obtidos por meio da aplicação das seguintes fórmulas:

$$LG = \frac{\text{Ativo Circulante} + \text{Realizável a Longo Prazo}}{\text{Passivo Circulante} + \text{Passivo Não Circulante}}$$

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante} + \text{Passivo Não Circulante}}$$

$$LC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$

10.4.4.4. Caso a empresa interessada apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) ou Liquidez Corrente (LC), será exigido, para fins de habilitação, patrimônio líquido mínimo de 10% (dez por cento) do valor total estimado da contratação.

10.4.4.5. Os indicadores fixados acima deverão ser atingidos em cada um dos 2 (dois) últimos exercícios sociais, sob pena de inabilitação.

10.4.4.6. Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos.

10.4.4.7. Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital — ECD ao Sped.

10.4.4.8. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura.

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

10.4.5. **Qualificação Técnica**

10.4.5.1. Comprovação de aptidão para o fornecimento de bens similares, de complexidade tecnológica e operacional equivalente ou superior à do objeto desta contratação, 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.

10.4.5.2. Para fins da comprovação de que trata este subitem, os atestados deverão demonstrar experiência anterior da licitante em fornecimento, implantação, configuração, ativação, suporte técnico ou garantia de solução corporativa de segurança da informação ou infraestrutura de rede, contemplando, no mínimo:

- a) fornecimento ou implantação de solução de firewall de próxima geração, switches, access points e XDR com licenciamento, suporte técnico, garantia ou atualizações;
- b) configuração, ativação, integração ou gerenciamento centralizado de solução de segurança de rede ou infraestrutura corporativa de TIC;
- c) prestação de suporte técnico, garantia, assistência técnica ou manutenção de solução corporativa de TIC, segurança da informação ou infraestrutura de rede.

10.4.5.3. Serão admitidos, para fins de comprovação dos requisitos mínimos exigidos, a apresentação e o somatório de diferentes atestados, desde que relativos a contratos executados de forma concomitante ou compatíveis com a complexidade tecnológica e operacional do objeto.

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

10.4.5.5. 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, local em que foi executado o objeto contratado, notas fiscais, ordens de fornecimento, termos de recebimento ou outros documentos idôneos.

10.4.5.6. Não se aplica a exigência de prova de atendimento a requisitos legais específicos adicionais, sem prejuízo da necessidade de atendimento integral às normas técnicas, regulatórias, ambientais, de segurança da informação, proteção de dados, garantia, suporte e licenciamento previstas neste Termo de Referência, no edital e na legislação aplicável.

10.4.6. Disposições gerais sobre habilitação

10.4.6.1. Quando permitida a participação de empresas estrangeiras que não funcionem no País, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados em tradução livre.

10.4.6.2. Na hipótese de o fornecedor ser empresa estrangeira que não funcione no País, para assinatura do contrato ou da ata de registro de preços ou do aceite do instrumento equivalente, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e apostilados nos termos do disposto no Decreto nº 8.660, de 29 de janeiro de 2016, ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

10.4.6.3. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

10.4.6.4. Se o fornecedor for a matriz, todos os documentos deverão estar em nome da matriz, e se o fornecedor for a filial, todos os documentos deverão estar em nome da filial, exceto para atestados de capacidade técnica, e no caso daqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

10.4.6.5. Serão aceitos registros de CNPJ de fornecedor matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

11. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

11.1. O custo estimado total da contratação, que corresponde ao valor máximo aceitável, é de R\$ 2.586.813,19 (dois milhões, quinhentos e oitenta e seis mil, oitocentos e treze reais e dezenove centavos), conforme custos unitários apostos na tabela contida no item 1.1 acima.

12. ADEQUAÇÃO ORÇAMENTÁRIA

12.1. As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento do Conselho Regional de Medicina do Estado de Minas Gerais para o exercício de 2026, na classificação abaixo:

6.2.2.1.2.44.90.52.004 - EQUIPAMENTOS DE INFORMÁTICA	R\$ 1.159.185,92
6.2.2.1.1.33.90.39.010 - MANUTENÇÃO DE SISTEMAS DE INFORMÁTICA - SOFTWARE	R\$ 735.199,62
6.2.2.1.1.33.90.39.045 - AQUISIÇÃO DE SISTEMAS/PROGRAMAS (SOFTWARE) DE INFORMÁTICA	R\$ 635.485,40
6.2.2.1.1.33.90.39.025 - SERVIÇOS DE SELEÇÃO, TREINAMENTO E APERFEIÇOAMENTO	R\$ 56.942,25

13. RESPONSÁVEIS

Alessandro de Freitas Bartels *Matheus Tadeu da Silveira Moreira* *Thiago da Fonseca Duarte*
Integrante Demandante **Integrante Administrativo** **Integrante Técnico**

14. APROVAÇÃO

Autoridade Máxima da Área de TIC
<i>Robertson Correia Bernardo</i> <i>Diretor do Departamento de Tecnologia da Informação</i>

15. ANEXO I - ESPECIFICAÇÕES TÉCNICAS

15.1. Requisitos essenciais da solução

15.1.1. Os equipamentos de hardware ofertados deverão ser novos, de primeiro uso, originais de fábrica, não reconicionados, não remanufaturados, não reformados e não previamente utilizados, devendo integrar a linha atual de comercialização e suporte do fabricante na data de apresentação da proposta.

15.1.2. Todos os equipamentos, softwares, licenças, subscrições, atualizações, garantias, suporte técnico e demais componentes necessários ao funcionamento da solução deverão possuir cobertura pelo período mínimo de 60 (sessenta) meses, contado do Termo de Recebimento Definitivo, conforme condições estabelecidas no Termo de Referência.

15.1.3. A licitante deverá comprovar a regularidade da origem, do licenciamento, da garantia, das atualizações e do suporte técnico dos produtos ofertados, mediante documentação oficial do fabricante, registro em portal, certificado de licenciamento, termo de ativação, entitlement, part number, declaração técnica, documentação de canal autorizado ou documento equivalente, quando aplicável, sem prejuízo da responsabilidade integral da Contratada pela execução do objeto.

15.1.4. Os produtos fornecidos deverão ser acompanhados de documentação técnica, manuais, guias de instalação, configuração e operação, em formato digital ou impresso, em

idioma português ou inglês, compatíveis com os equipamentos, softwares, licenças, subscrições e demais componentes ofertados.

15.1.5. O prazo máximo para entrega dos equipamentos, licenças, subscrições e demais componentes necessários à solução será de até 90 (noventa) dias corridos, contado do recebimento da Ordem de Fornecimento de Bens — OFB pela Contratada, devendo a entrega ocorrer, como regra, na Sede do CRM-MG, em Belo Horizonte/MG, salvo disposição diversa expressamente indicada pela Contratante.

15.1.6. A comprovação da capacidade técnica da licitante deverá observar as exigências previstas no item de Qualificação Técnica do Termo de Referência, especialmente quanto à apresentação de atestados de capacidade técnica compatíveis com o objeto da contratação.

15.1.7. A Contratada deverá comprovar, antes do início das atividades técnicas correspondentes, que dispõe de profissional ou equipe técnica com certificação oficial do fabricante para instalação, configuração, ativação, integração, suporte técnico e transferência de conhecimento da solução ofertada, admitida a comprovação por meio de certificação técnica oficial do fabricante, certificado de treinamento, declaração do fabricante, vínculo profissional, contrato de prestação de serviços, declaração de disponibilidade ou documento equivalente.

15.1.8. Toda solução deve estar consoante com os demais itens deste Termo de Referência.

15.2. Quantitativo dos itens

Item	Descrição	Quantidade
1	Equipamento de gerenciamento centralizado (Appliance)	1
2	Firewall Tipo 1	2
3	Firewall Tipo 2	20
4	Switch Gigabit de 8 Portas com PoE	7
5	Switch Gigabit de 16 Portas	20
6	Access Point Interno Tipo 1	30
7	Access Point Interno Tipo 2	20
8	Solução de Detecção e Resposta Estendida (XDR)	330
9	Licenciamento, Atualizações, Suporte (24x7) do Fabricante e Garantia de 60 Meses para Toda a Solução	1
10	Instalação e Configuração da Solução	1
11	Treinamento Oficial do Fabricante em Cada Produto Fornecido para uma Turma de até 2 Participantes	1

15.3. ITEM 1 - EQUIPAMENTO DE GERENCIAMENTO CENTRALIZADO (Appliance)

15.3.1. Gerenciamento Unificado

15.3.1.1. Deve ser fornecido como um dispositivo físico (Appliance) com os seguintes atributos:

15.3.1.1.1. Formato de montagem em Rack com tamanho 2U.

- 15.3.1.1.2. Capacidade de armazenamento utilizável de 24TB.
- 15.3.1.1.3. Nível de RAID 50 como padrão.
- 15.3.1.1.4. Inclusão de 04 (quatro) interfaces 1GE RJ-45.
- 15.3.1.1.5. Inclusão de 02 (duas) interfaces 1GE SFP.
- 15.3.1.1.6. Deve possuir capacidade licenciada para controlar até 150 dispositivos.
- 15.3.1.1.7. Deve ser inteiramente compatível e proveniente do mesmo fabricante que os itens 2, 3, 4, 5, 6 e 7 deste edital.

15.3.2. **Funções do Sistema de Gerenciamento**

- 15.3.2.1. Na data de apresentação da proposta, nenhum dos modelos ofertados pode estar listado no site do fabricante nas listas de fim de vida útil (end-of-life) e nem de fim de vendas (end-of-sale).
- 15.3.2.2. O controle da solução deve suportar acesso por meio de SSH e interface WEB (HTTPS).
- 15.3.2.3. Deve ser possível o acesso simultâneo de múltiplos administradores.
- 15.3.2.4. Deve incluir uma interface baseada em linha de comando para a administração do sistema de gerência.
- 15.3.2.5. Deve incorporar um mecanismo de pesquisa de comandos no gerenciamento via SSH, facilitando a localização.
- 15.3.2.6. Deve haver bloqueio de alterações no caso de acesso simultâneo por dois ou mais administradores.
- 15.3.2.7. Possibilidade de definir perfis de acesso ao console com permissões detalhadas, incluindo acesso de escrita, acesso de leitura, criação de usuários e modificação de configurações.
- 15.3.2.8. Capacidade de gerar alertas automáticos via Email.
- 15.3.2.9. Capacidade de gerar alertas automáticos via SNMP.
- 15.3.2.10. Capacidade de gerar alertas automáticos via Syslog.
- 15.3.2.11. Deve suportar XML API.
- 15.3.2.12. O sistema de gerência deve permitir a criação e gestão de políticas de firewall e controle de aplicação.
- 15.3.2.13. O sistema de gerência deve permitir a criação e gestão de políticas de IPS, Antivírus e Anti-Spyware.
- 15.3.2.14. O sistema de gerência deve permitir a criação e gestão de políticas de Filtro de URL.
- 15.3.2.15. Permitir a localização de quais regras estão utilizando um determinado objeto.
- 15.3.2.16. Deve atribuir um número sequencial a cada regra de firewall.
- 15.3.2.17. Deve atribuir um número sequencial a cada regra de NAT.
- 15.3.2.18. Deve atribuir um número sequencial a cada regra de QOS.
- 15.3.2.19. Deve atribuir um número sequencial a cada regra de DOS.
- 15.3.2.20. Permitir a criação de regras que se tornem ativas em horários predefinidos.
- 15.3.2.21. Permitir a criação de regras com uma data de validade (expiração).
- 15.3.2.22. Permitir o backup das configurações e a opção de reverter (rollback) para a última configuração salva.
- 15.3.2.23. Deve possuir um mecanismo para validar políticas, alertando sobre regras que ofusquem ou entrem em conflito com outras (shadowing).
- 15.3.2.24. Deve permitir a visualização e comparação entre configurações atuais, anteriores e antigas.

- 15.3.2.25. Deve permitir que todos os firewalls sejam administrados de forma centralizada utilizando um único servidor de gerência.
- 15.3.2.26. Um sistema de backup/restauração para todas as configurações da solução de gerência deve ser incluso, permitindo ao administrador agendar backups em dias e horários específicos.
- 15.3.2.27. O administrador deve ser autorizado a transferir os backups para um servidor FTP.
- 15.3.2.28. O administrador deve ser autorizado a transferir os backups para um servidor SCP.
- 15.3.2.29. Caso os appliances percam a conexão com os servidores de gerência, os firewalls devem continuar processando o tráfego sem interrupções.
- 15.3.2.30. A solução deve incluir uma ferramenta para gerenciamento centralizado das licenças de todos os appliances controlados, permitindo ao administrador a atualização das licenças através dessa ferramenta.
- 15.3.2.31. A solução deve possibilitar a instalação remota e centralizada de novas versões de software nos appliances.
- 15.3.2.32. Os administradores devem poder se autenticar nos servidores de gerência usando contas de usuários LOCAIS.
- 15.3.2.33. Deve ser permitido que os administradores se autenticuem usando usuários de base externa LDAP.
- 15.3.2.34. Deve ser permitido que os administradores se autenticuem usando base externa RADIUS.
- 15.3.2.35. Deve ser permitido que os administradores se autenticuem usando Certificado Digital X.509 (PKI).
- 15.3.2.36. Deve suportar a sincronização do relógio interno via protocolo NTP.
- 15.3.2.37. Deve registrar todas as tentativas ou logins bem-sucedidos de qualquer usuário.
- 15.3.2.38. Os registros de auditoria para configurações de regras e objetos devem ser visualizados em uma lista separada dos registros relacionados ao tráfego de dados.
- 15.3.2.39. Devem ser fornecidos manuais de instalação, configuração e operação de toda a solução, em português ou inglês, com excelente qualidade de apresentação.
- 15.3.2.40. Deve ser capaz de gerar relatórios ou exibir comparativos entre duas sessões distintas, resumindo todas as alterações realizadas.
- 15.3.2.41. Suportar SNMP versão 2 e versão 3 nos equipamentos de gerência.
- 15.3.2.42. Deve permitir habilitar e desabilitar as permissões de acesso (HTTP, HTTPS, SSH, SNMP e Telnet) para cada interface de rede da solução de gerência.
- 15.3.2.43. Deve permitir a virtualização da solução de gerência, de forma que cada administrador possa controlar, visualizar e modificar apenas os dispositivos autorizados em seu ambiente virtualizado.
- 15.3.2.44. A solução de gerência deve permitir a criação de administradores com acesso a todas as instâncias de virtualização.
- 15.3.2.45. Permitir a importação de eventuais políticas e objetos já existentes nos dispositivos ao adicioná-los à solução de gerência.
- 15.3.2.46. Permitir a visualização, a partir da estação de gerência centralizada, de informações detalhadas dos dispositivos como licenças, horário do sistema e firmware.
- 15.3.2.47. Permitir a criação de modelos de configuração (templates) na solução de gerência para dispositivos, englobando informações de DNS, SNMP, Configurações de LOG e Administração.
- 15.3.2.48. Permitir a criação centralizada dos objetos que serão empregados nas políticas.

15.4. ITENS 2 E 3 - FIREWALL TIPO 1 E FIREWALL TIPO 2 -

15.4.1. Exigências mínimas de funcionalidades técnicas

15.4.1.1. A solução deve consistir em uma plataforma de proteção de rede baseada em um appliance, com recursos de Next Generation Firewall (NGFW), e incluir um console de gerência e monitoração.

15.4.1.2. Os recursos de NGFW incluem: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.

15.4.1.3. As funções de proteção de rede podem funcionar em múltiplos appliances, contanto que cumpram integralmente todos os requisitos desta especificação.

15.4.1.4. A plataforma deve ser otimizada para a inspeção de conteúdo de aplicações na camada 7.

15.4.1.5. O gerenciamento da solução deve suportar acesso via SSH, cliente dedicado ou WEB (HTTPS) e API aberta.

15.4.1.6. Os dispositivos de proteção de rede devem suportar 200 VLAN Tags 802.1q.

15.4.1.7. Os dispositivos de proteção de rede devem suportar roteamento baseado em política (Policy based routing) ou encaminhamento baseado em política (policy based forwarding).

15.4.1.8. Os dispositivos de proteção de rede devem suportar roteamento multicast (PIM-SM e PIM-DM).

15.4.1.9. Os dispositivos de proteção de rede devem suportar DHCP Relay.

15.4.1.10. Os dispositivos de proteção de rede devem suportar DHCP Server.

15.4.1.11. Os dispositivos de proteção de rede devem suportar Jumbo Frames.

15.4.1.12. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet lógicas.

15.4.1.13. Deve suportar NAT dinâmico (Many-to-Many).

15.4.1.14. Deve suportar NAT estático (1-to-1).

15.4.1.15. Deve suportar NAT estático bidirecional 1-to-1.

15.4.1.16. Deve suportar Tradução de porta (PAT).

15.4.1.17. Deve suportar NAT de Origem.

15.4.1.18. Deve suportar NAT de Destino.

15.4.1.19. Deve suportar NAT de Origem e NAT de Destino em simultâneo.

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

15.4.1.21. Deve suportar NAT64 e NAT46.

15.4.1.22. Deve implementar o protocolo ECMP.

15.4.1.23. Deve implementar balanceamento de link por hash do IP de origem.

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

15.4.1.25. Deve implementar balanceamento de link por peso, permitindo definir o percentual de tráfego que será escoado por cada link. Deve suportar o balanceamento de, no mínimo, três links.

15.4.1.26. Deve implementar balanceamento de links sem a necessidade de criar zonas ou utilizar instâncias virtuais.

15.4.1.27. A solução deve prover recursos de roteamento inteligente, determinando o melhor caminho para uma aplicação com base em regras predefinidas.

15.4.1.28. A solução deve ser capaz de monitorar e detectar falhas através da associação de health check, permitindo testes de resposta por ping, http, tcp/udp echo e twamp.

- 15.4.1.29. Deve ser permitida a criação de políticas de roteamento baseadas em: latência, jitter, perda de pacote, banda ocupada ou todos ao mesmo tempo.
- 15.4.1.30. Devem estar disponíveis diversas maneiras de escolher o link, incluindo: melhor link, menor custo e definição de níveis máximos de qualidade aceitáveis para o uso desses links em um roteamento de aplicação.
- 15.4.1.31. A solução deve fornecer estatísticas em tempo real sobre a ocupação de banda (upload e download) e o desempenho do health check (packet loss, jitter e latência).
- 15.4.1.32. Além de permitir a definição de banda máxima e garantida por aplicação, deve também suportar a correspondência em categorias de URL, IPs de origem e destino, logins e portas.
- 15.4.1.33. Deve possibilitar roteamento diferenciado dependendo do grupo de usuário selecionado na regra.
- 15.4.1.34. Deve permitir o monitoramento via SNMP de falhas de hardware, CPU, memória, segurança e interfaces.
- 15.4.1.35. Deve enviar logs para sistemas de monitoração externos, simultaneamente.
- 15.4.1.36. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL.
- 15.4.1.37. Proteção anti-spoofing.
- 15.4.1.38. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2).
- 15.4.1.39. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3).
- 15.4.1.40. Suportar OSPF graceful restart.
- 15.4.1.41. Deve suportar Modo Sniffer, para inspeção do tráfego de dados da rede através de porta espelhada.
- 15.4.1.42. Deve suportar Modo Camada - 2 (L2), para inspeção de dados em linha e visibilidade do tráfego.
- 15.4.1.43. Deve suportar Modo Camada - 3 (L3), para inspeção de dados em linha e visibilidade do tráfego.
- 15.4.1.44. Suporte para configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo em modo transparente.
- 15.4.1.45. Suporte para configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo em layer 3.
- 15.4.1.46. Suporte para configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo em layer 3 com, no mínimo, 3 equipamentos no cluster.
- 15.4.1.47. A configuração em alta disponibilidade deve sincronizar Sessões.
- 15.4.1.48. A configuração em alta disponibilidade deve sincronizar Configurações, incluindo (mas não se limitando a) políticas de Firewall, NAT, QOS e objetos de rede.
- 15.4.1.49. Configuração em alta disponibilidade deve sincronizar Associações de Segurança das VPNs.
- 15.4.1.50. A configuração em alta disponibilidade deve sincronizar Tabelas FIB.
- 15.4.1.51. O HA (modo de Alta-Disponibilidade) deve permitir a monitoração de falha de link.
- 15.4.1.52. Deve possuir suporte para a criação de sistemas virtuais no mesmo appliance.
- 15.4.1.53. Em alta disponibilidade, deve ser possível utilizar clusters virtuais (ativo-ativo ou ativo-passivo), permitindo a distribuição de carga entre diferentes contextos.
- 15.4.1.54. Deve permitir a criação de administradores independentes para cada sistema virtual, possibilitando que contextos virtuais sejam administrados por equipes distintas.
- 15.4.1.55. Controle por Política de Firewall.

- 15.4.1.56. Deve suportar controles por zona de segurança.
- 15.4.1.57. Controles de políticas por porta e protocolo.
- 15.4.1.58. Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento) e categorias de aplicações.
- 15.4.1.59. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.
- 15.4.1.60. Controle de políticas por código de País (Ex: BR, USA, UK).
- 15.4.1.61. Deve descriptografar tráfego de saída (Outbound) em conexões negociadas com TLS 1.2.
- 15.4.1.62. Controle de inspeção e descriptografia de SSH por política.
- 15.4.1.63. Deve permitir o bloqueio de arquivo por sua extensão e ser capaz de identificar corretamente o tipo do arquivo mesmo que a extensão seja renomeada.
- 15.4.1.64. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo).
- 15.4.1.65. QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações.
- 15.4.1.66. Suporte a objetos e regras IPV6.
- 15.4.1.67. Suporte a objetos e regras multicast.
- 15.4.1.68. Deve suportar no mínimo dois tipos de resposta nas políticas de firewall: Drop sem notificação, Drop com notificação, Drop com opção de envio de ICMP Unreachable para a origem, TCP-Reset para o cliente, TCP-Reset para o servidor ou para ambos os lados da conexão.
- 15.4.1.69. Deve suportar o agendamento de políticas para ativá-las e desativá-las automaticamente em horários pré-definidos.
- 15.4.2. **Controle de Aplicações**
- 15.4.2.1. Os dispositivos de proteção de rede devem ter a capacidade de identificar aplicações, independente da porta e protocolo.
- 15.4.2.2. Deve ser possível permitir ou bloquear unicamente aplicações sem a necessidade de liberar portas e protocolos.
- 15.4.2.3. Deve reconhecer pelo menos 1700 aplicações distintas, incluindo, mas não limitado a: tráfego peer-to-peer, redes sociais, acesso remoto, atualização de software, protocolos de rede, VoIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos e e-mail.
- 15.4.2.4. Deve reconhecer, no mínimo, 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.
- 15.4.2.5. Deve inspecionar o conteúdo (payload) do pacote de dados para detectar assinaturas de aplicações conhecidas, independentemente de porta e protocolo.
- 15.4.2.6. Deve identificar o uso de táticas evasivas, possibilitando a visualização e controle de aplicações e ataques que empregam criptografia evasiva, como Skype e a rede Tor.
- 15.4.2.7. Deve realizar a decodificação de protocolos para identificar aplicações encapsuladas e verificar a conformidade do tráfego com a especificação do protocolo (ex: Yahoo Instant Messenger usando HTTP). A decodificação também deve identificar funcionalidades específicas dentro de uma aplicação (ex: compartilhamento de arquivo no Webex).
- 15.4.2.8. Identificar táticas evasivas que utilizam comunicações criptografadas.

- 15.4.2.9. Atualizar automaticamente a base de assinaturas de aplicações.
- 15.4.2.10. Limitar a largura de banda (traffic shaping) usada por aplicações (download/upload), baseado em IP de origem, usuários e grupos.
- 15.4.2.11. Os dispositivos de proteção de rede devem ter a capacidade de identificar o usuário de rede através da integração com o Microsoft Active Directory, sem precisar instalar agentes no Domain Controller ou nas estações dos usuários.
- 15.4.2.12. Deve ser possível aplicar o controle de aplicações em múltiplas regras de segurança do dispositivo, não se restringindo a um número limitado de regras.
- 15.4.2.13. Deve suportar múltiplos métodos de identificação e classificação das aplicações, utilizando pelo menos checagem de assinaturas e decodificação de protocolos.
- 15.4.2.14. Para segurança eficiente, deve ser capaz de controlar aplicações desconhecidas, não se limitando apenas às aplicações conhecidas.
- 15.4.2.15. Deve permitir a criação nativa de assinaturas personalizadas para aplicações proprietárias diretamente na interface gráfica, sem depender de ações do fabricante.
- 15.4.2.16. A criação de assinaturas personalizadas deve suportar o uso de expressões regulares, contexto (sessões ou transações), posição no payload dos pacotes TCP e UDP, e decodificadores de pelo menos os seguintes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, RTSP e SSL.
- 15.4.2.17. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas.
- 15.4.2.18. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc.), oferecendo controle/políticas granularizadas.
- 15.4.2.19. Deve possibilitar a diferenciação de tráfegos de Mensagens Instantâneas (AIM, Hangouts, Facebook Chat, etc.), oferecendo controle/políticas granularizadas.
- 15.4.2.20. Deve possibilitar a diferenciação e controle de subcomponentes das aplicações, como permitir o chat Hangouts e bloquear a chamada de vídeo.
- 15.4.2.21. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc.), oferecendo controle/políticas granularizadas.
- 15.4.2.22. Deve permitir a criação de grupos dinâmicos de aplicações baseados em características como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc).
- 15.4.2.23. Deve permitir a criação de grupos dinâmicos de aplicações baseados em características como: Nível de risco da aplicação.
- 15.4.2.24. Deve permitir a criação de grupos estáticos de aplicações baseados em características como: Categoria da aplicação.

15.4.3. **Prevenção de Ameaças**

- 15.4.3.1. Os dispositivos de proteção devem ter módulos de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall para proteger contra-ataques.
- 15.4.3.2. Deve incluir assinaturas para prevenção de intrusão (IPS) e para bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware).
- 15.4.3.3. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar permanentemente, mesmo que o direito a atualizações ou o contrato de garantia de software com o fabricante expire.
- 15.4.3.4. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando a alta disponibilidade estiver implementada.
- 15.4.3.5. Deve implementar as seguintes ações para ameaças detectadas pelo IPS: permitir, permitir e registrar, bloquear, bloquear o IP do atacante por um período e enviar tcp-reset.
- 15.4.3.6. As assinaturas podem ser ativadas ou desativadas, ou habilitadas apenas para monitoração.

- 15.4.3.7. Deve ser possível criar políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança.
- 15.4.3.8. É obrigatória a possibilidade de exceções por IP de origem ou de destino nas regras, ou por assinatura individual.
- 15.4.3.9. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, permitindo diferentes configurações de política por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação desses elementos.
- 15.4.3.10. Deve permitir o bloqueio de vulnerabilidades.
- 15.4.3.11. Deve permitir o bloqueio de exploits conhecidos.
- 15.4.3.12. Deve incluir proteção contra ataques de negação de serviços.
- 15.4.3.13. Deve possuir o seguinte mecanismo de inspeção de IPS: Análise de padrões de estado de conexões.
- 15.4.3.14. Deve possuir o seguinte mecanismo de inspeção de IPS: Análise de decodificação de protocolo.
- 15.4.3.15. Deve possuir o seguinte mecanismo de inspeção de IPS: Análise para detecção de anomalias de protocolo.
- 15.4.3.16. Deve possuir o seguinte mecanismo de inspeção de IPS: Análise heurística.
- 15.4.3.17. Deve possuir o seguinte mecanismo de inspeção de IPS: IP Defragmentation.
- 15.4.3.18. Deve possuir o seguinte mecanismo de inspeção de IPS: Remontagem de pacotes de TCP.
- 15.4.3.19. Deve possuir o seguinte mecanismo de inspeção de IPS: Bloqueio de pacotes malformados.
- 15.4.3.20. Deve ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc.
- 15.4.3.21. Deve detectar e bloquear a origem de portscans.
- 15.4.3.22. Deve bloquear ataques realizados por worms conhecidos.
- 15.4.3.23. Deve possuir assinaturas específicas para mitigar ataques DoS e DDoS.
- 15.4.3.24. Deve possuir assinaturas para bloqueio de ataques de buffer overflow.
- 15.4.3.25. Deve possibilitar a criação de assinaturas customizadas através da interface gráfica do produto.
- 15.4.3.26. Deve permitir o uso de operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações.
- 15.4.3.27. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3.
- 15.4.3.28. Deve identificar e bloquear comunicação com botnets.
- 15.4.3.29. Deve registrar no console de monitoração as seguintes informações sobre ameaças identificadas: nome da assinatura ou do ataque, aplicação, usuário, origem e destino da comunicação, além da ação tomada.
- 15.4.3.30. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou por filtro pré-definido.
- 15.4.3.31. Deve possuir a função de proteção na resolução de endereços via DNS, identificando requisições de nomes para domínios maliciosos de botnets conhecidas.
- 15.4.3.32. Os eventos devem identificar o país de onde a ameaça se originou.
- 15.4.3.33. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.
- 15.4.3.34. Possuir proteção contra downloads involuntários (usando HTTP) de arquivos executáveis e maliciosos.

15.4.3.35. Deve ser possível a configuração de diferentes políticas de controle de ameaças baseadas nas políticas do firewall, considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc., ou seja, cada política de firewall pode ter uma configuração distinta de IPS.

15.4.4. **Filtro de URL**

15.4.4.1. Permite especificar política por tempo, definindo regras para um horário ou período específico (dia, mês, ano, dia da semana e hora).

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

15.4.4.3. Deve ter a capacidade de criar políticas baseadas na visibilidade e controle de quais URLs estão sendo utilizadas por quem, através da integração com serviços de diretório, Active Directory e base de dados local.

15.4.4.4. Deve suportar a capacidade de criar políticas baseadas no controle por URL e categoria de URL.

15.4.4.5. Deve possuir pelo menos 60 categorias de URLs.

15.4.4.6. Deve possuir a função de excluir URLs do bloqueio, por categoria.

15.4.4.7. Permitir a personalização da página de bloqueio.

15.4.4.8. Permitir o bloqueio com opção de continuação (o usuário pode acessar um site potencialmente bloqueado confirmando na tela de bloqueio e usando um botão "Continuar").

15.4.5. **Identificação de Usuários**

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

15.4.5.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos, permitindo controle/políticas granularizadas.

15.4.5.3. Deve possuir integração e suporte ao Microsoft Active Directory para o Windows Server 2019 e posteriores.

15.4.5.4. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos, permitindo controle granularizado e suportando single sign-on. Esta funcionalidade não deve ter limites licenciados de usuários ou qualquer restrição de uso (como uso de sistemas virtuais, segmentos de rede, etc.).

15.4.5.5. Deve possuir integração com Radius para identificação de usuários e grupos, permitindo controle/políticas granularizadas.

15.4.5.6. Deve possuir integração com LDAP para identificação de usuários e grupos, permitindo controle/políticas granularizadas.

15.4.5.7. Deve permitir o controle sem a instalação de cliente de software, em equipamentos que solicitam acesso à internet, através de um portal de autenticação (Captive Portal) residente no firewall.

15.4.5.8. Deve suportar a identificação de múltiplos usuários conectados no mesmo endereço IP em ambientes Microsoft Terminal Server, possibilitando visibilidade e controle granular por usuário sobre o uso das aplicações nesses serviços.

15.4.5.9. Deve permitir a criação de grupos customizados de usuários no firewall, baseados em atributos do LDAP/AD.

15.4.5.10. Permitir integração com tokens para autenticação de usuários, incluindo (mas não limitado a) acesso à internet e gerenciamento da solução.

15.4.5.11. Deve prover pelo menos um token nativamente, possibilitando autenticação de duplo fator.

15.4.6. **QoS e Traffic Shaping**

- 15.4.6.1. Para controlar aplicações e tráfego com consumo excessivo (como youtube, ustream, etc.), a solução deve ser capaz de, além de permitir ou negar, controlar essas aplicações por políticas de largura de banda máxima. Isso se aplica a diferentes usuários ou aplicações, incluindo streaming de áudio e vídeo.
- 15.4.6.2. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem.
- 15.4.6.3. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino.
- 15.4.6.4. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo.
- 15.4.6.5. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações.
- 15.4.6.6. Suportar a criação de políticas de QoS e Traffic Shaping por porta.
- 15.4.6.7. O QoS deve permitir a definição de tráfego com banda garantida.
- 15.4.6.8. O QoS deve permitir a definição de tráfego com banda máxima.
- 15.4.6.9. O QoS deve permitir a definição de fila de prioridade.
- 15.4.6.10. Suportar a priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.
- 15.4.6.11. Suportar a marcação de pacotes Diffserv, inclusive por aplicação.
- 15.4.6.12. Deve disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping.
- 15.4.7. **Filtro de Dados**
- 15.4.7.1. Permitir identificar e, opcionalmente, impedir a transferência de vários tipos de arquivos (MS Office, PDF, etc.) identificados sobre aplicações (HTTP, FTP, SMTP, etc.).
- 15.4.7.2. Suportar a identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses arquivos.
- 15.4.7.3. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses arquivos.
- 15.4.7.4. 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.
- 15.4.8. **Geolocalização**
- 15.4.8.1. Suportar a criação de políticas por geolocalização, permitindo o bloqueio do tráfego proveniente de determinado(s) País/Países.
- 15.4.8.2. Deve possibilitar a visualização dos países de origem e destino nos logs de acesso.
- 15.4.8.3. Deve possibilitar a criação de regiões geográficas pela interface gráfica para uso em políticas.
- 15.4.9. **VPN**
- 15.4.9.1. Suportar VPN Site-to-Site e Client-To-Site.
- 15.4.9.2. Suportar IPSec VPN.
- 15.4.9.3. A VPN IPSEc deve suportar 3DES.
- 15.4.9.4. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1.
- 15.4.9.5. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14.
- 15.4.9.6. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2).
- 15.4.9.7. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard).
- 15.4.9.8. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI.
- 15.4.9.9. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall.
- 15.4.9.10. Deve permitir habilitar e desabilitar túneis de VPN IPSEC na interface gráfica,

facilitando o troubleshooting.

15.4.9.11. Deve garantir que todo o tráfego dos usuários remotos de VPN seja direcionado para dentro do túnel, impedindo comunicação direta com dispositivos locais como proxies.

15.4.9.12. Atribuição de DNS nos clientes remotos de VPN.

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

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

15.4.9.15. Deve permitir que a conexão com a VPN seja estabelecida: Antes da autenticação do usuário na estação.

15.4.9.16. Deve permitir que a conexão com a VPN seja estabelecida: Após a autenticação do usuário na estação.

15.4.9.17. Deve permitir que a conexão com a VPN seja estabelecida: Sob demanda do usuário.

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

15.4.9.19. O cliente IPSEC client-to-site deve ser compatível com pelo menos: Windows 10 e superiores (32 e 64 bit) e Mac OS X (v10.10 e superiores).

15.4.10. **Funções de Balanceamento de Carga (SD-WAN) para os Links Remotos**

15.4.10.1. A solução SD-WAN deve ser provida com recursos de segurança integrados: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.

15.4.10.2. A solução SD-WAN deve suportar micro-segmentação de tráfego, permitindo a aplicação de políticas de IPS e Antivírus entre segmentos de LAN.

15.4.10.3. A solução SD-WAN deve suportar NAT em contexto de saída (NAT Outbound) para um pool de IPs públicos.

15.4.10.4. A solução deve ser capaz de fornecer a função Zero Touch Provisioning.

15.4.10.5. A solução deve suportar ADVPN entre o Ponto Central e as Unidades Remotas.

15.4.10.6. A configuração VPN IPsec deve suportar a versão IKE v2.0.

15.4.10.7. A configuração VPN IPsec deve suportar DH Group 14 e 15.

15.4.10.8. A solução deve suportar os seguintes protocolos: IPv6, VRRP ou Equivalente, VRF, BGP, OSPF, RIPv2, 802.1Q, BFD, Dynamic Multipath, Policy Based Routing.

15.4.10.9. Reconhecimento em camada 7 totalmente independente da camada 4.

15.4.10.10. Deve, alternativamente, incluir um banco de dados interno onde seja possível associar uma aplicação a um determinado IP ou faixa de IPs de destino.

15.4.10.11. O reconhecimento de aplicações deve ser atualizado dinamicamente e de forma transparente para o dispositivo.

15.4.10.12. O reconhecimento de aplicações deve ser realizado independentemente de porta e protocolo, através da inspeção do payload do pacote de dados.

15.4.10.13. No que diz respeito ao reconhecimento de Aplicações, a solução deve fornecer o reconhecimento padrão em camada 7 de, pelo menos, mais de 1.000 aplicações amplamente utilizadas em contextos de SaaS, Aplicações na Nuvem e Aplicações Multimídia (Vimeo, YouTube, Facebook, entre outros).

15.4.10.14. A solução deve ser capaz de ajustar suas políticas de SDWAN (manual ou automaticamente) em condições de modificação da largura de banda.

15.4.10.15. A solução deve ser capaz de avaliar o Status de Saúde do Link com base em critérios mínimos de: Latência, Jitter e packet loss. Deve ser possível configurar um valor limite (threshold) para cada item, que servirá como fator de decisão nas regras de SD-WAN.

15.4.10.16. A solução deve permitir modificar o tempo de checagem (em segundos) para cada um dos links.

15.4.10.17. A solução deve permitir a configuração de políticas de QoS em camada 7,

associadas percentualmente à largura de banda da Interface SD-WAN.

15.4.10.18. A solução deve permitir a configuração de políticas de QoS em valores onde o máximo corresponde à totalidade da largura de banda disponível no equipamento.

15.4.10.19. A solução deve possibilitar a distribuição de peso nos links que compõem o SDWAN, conforme critério do usuário. O algoritmo de balanceamento pode ser baseado em: Número de Sessões, Volume de Tráfego, IP de Origem e Destino, e Transbordo de Link (Spillover).

15.4.10.20. A Alta Disponibilidade (HA) provida pela solução de SD-WAN (física ou virtual) deve atender aos seguintes critérios: Suportar Balanceamento Ativo Ativo, Suportar Balanceamento Ativo Passivo, Suportar Balanceamento de até 4 peers.

15.4.10.21. A solução SD-WAN deve oferecer ferramentas de diagnóstico (troubleshooting) em console de linha de comando ou gráfica. Estas devem permitir: executar Packet sniffer para tráfego específico (filtrando por IP e Porta) e realizar debug detalhado das fases de negociação VPN.

15.4.10.22. A solução SD-WAN deve suportar marcação de pacotes DSCP nas definições e regras de tráfego.

15.5. **ITEM 2 - FIREWALL TIPO 1**

15.5.1. **Características Específicas**

15.5.1.1. Taxa de transferência (Throughput) de, no mínimo, 26 Gbps com a função de firewall ativa, independentemente do tamanho do pacote.

15.5.1.2. Suporte a, no mínimo, 10.500.000 conexões simultâneas.

15.5.1.3. Suporte a, no mínimo, 350.000 novas conexões por segundo.

15.5.1.4. Throughput de VPN IPSec de, no mínimo, 32 Gbps.

15.5.1.5. Deve estar licenciado para, ou suportar sem licença, 2.000 túneis de VPN IPSEC Site-to-Site simultâneos.

15.5.1.6. Deve estar licenciado para, ou suportar sem licença, 15.000 túneis de clientes VPN IPSEC simultâneos.

15.5.1.7. Suportar no mínimo 9 Gbps de throughput de IPS.

15.5.1.8. Suporte a, no mínimo, 26 Gbps de throughput de Application Control.

15.5.1.9. Suportar no mínimo 7 Gbps de throughput de Inspeção SSL.

15.5.1.10. Throughput de, no mínimo 6 Gbps com as seguintes funcionalidades ativadas simultaneamente para todas as assinaturas: controle de aplicação, IPS, Antivírus e Antispyware.

15.5.1.11. Deve possuir pelo menos 8 interfaces 1/10 GE SFP+/SFP.

15.5.1.12. Deve possuir pelo menos 8 interfaces 1 GE RJ-45.

15.5.1.13. Deve possuir pelo menos 8 interfaces 1 / 2.5 / 5 GE RJ-45.

15.5.1.14. Deve possuir pelo menos 4 interfaces 1 GE SFP.

15.5.1.15. Estar licenciado para, ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance.

15.5.2. **Condições operacionais**

15.5.2.1. Alimentação Dupla / tensão de 100-240 VAC.

15.5.2.2. Alimentação Dupla / frequência de 50/60 Hz.

15.5.2.3. Temperatura - faixa de operação de 0º a 40º C.

15.5.2.4. Cada appliance deve ser fornecido com 2 (duas) fontes de alimentação redundantes.

15.6. **ITEM 3 - FIREWALL TIPO 2**

15.6.1. **Características Específicas**

- 15.6.1.1. Throughput de, no mínimo, 3.5 Gbps com a funcionalidade de firewall ativada.
- 15.6.1.2. Suporte a, no mínimo, 550.000 conexões simultâneas.
- 15.6.1.3. Suporte a, no mínimo, 30.000 novas conexões por segundo.
- 15.6.1.4. Throughput de VPN IPSec de, no mínimo, 3.5 Gbps.
- 15.6.1.5. Deve estar licenciado para, ou suportar sem licença, 200 túneis de VPN IPSEC Site-to-Site simultâneos.
- 15.6.1.6. Deve estar licenciado para, ou suportar sem licença, 250 túneis de clientes VPN IPSEC simultâneos.
- 15.6.1.7. Suportar no mínimo 800 Mbps de throughput de IPS.
- 15.6.1.8. Suporte a, no mínimo, 800 Mbps de throughput de Application Control.
- 15.6.1.9. Suportar no mínimo 300 Mbps de throughput de Inspeção SSL.
- 15.6.1.10. Throughput de, no mínimo 500 Mbps com as seguintes funcionalidades ativadas simultaneamente para todas as assinaturas: controle de aplicação, IPS, Antivírus e Antispyware.
- 15.6.1.11. Se o fabricante divulgar múltiplos números de desempenho para qualquer funcionalidade, somente o menor valor será aceito.
- 15.6.1.12. Deve possuir pelo menos 4 interfaces 1 GE RJ-45.

15.6.2. **Condições operacionais**

- 15.6.2.1. Alimentação Dupla / tensão de 100-240 VAC.
- 15.6.2.2. Alimentação Dupla / frequência de 50/60 Hz.
- 15.6.2.3. Temperatura - faixa de operação de 0º a 40º C.

15.7. **ITEM 4 - SWITCH GIGABIT 8 PORTAS POE**

15.7.1. **Características Gerais**

- 15.7.1.1. Deve ser fornecido com no mínimo 08 portas 1 GbE RJ-45 com PoE.
- 15.7.1.2. Deve ser fornecido com no mínimo 2 slots 1 GbE SFP.
- 15.7.1.3. Deve possuir 1 interface RJ-45 ou serial para acesso console local.
- 15.7.1.4. Deve possuir Certificado de Homologação na Anatel, de acordo com a Resolução nº 242.
- 15.7.1.5. Deve possuir alimentação interna 110/220VAC 50/60Hz.
- 15.7.1.6. Deve disponibilizar no mínimo 65W para alimentação PoE.
- 15.7.1.7. Deve suportar os padrões PoE 802.3af/at.
- 15.7.1.8. Deve ser compatível com os itens 1, 2 e 3 deste edital para fins de gerenciamento centralizado.
- 15.7.1.9. Não serão aceitos equipamentos cujo fabricante tenha anunciado o fim de vendas do modelo (End of Sales).

15.7.2. **Controle**

- 15.7.2.1. Deve possuir tabela para 8.000 (oito mil) endereços MAC.
- 15.7.2.2. Deve possuir capacidade de encaminhamento de no mínimo 30 Mpps.
- 15.7.2.3. Deve possuir capacidade de comutação de no mínimo 20 Gbps.
- 15.7.2.4. Deve suportar no mínimo 4.000 VLANs.
- 15.7.2.5. Deve suportar 8 grupos de agregação de links (padrão IEEE 802.3ad), permitindo

até 8 links Gigabit Ethernet por grupo.

15.7.2.6. Deve possuir no mínimo 256 MB de memória RAM.

15.7.2.7. Deve possuir memória flash de no mínimo 32MB.

15.7.2.8. Deve suportar no mínimo 640 ACLs.

15.7.2.9. Deve suportar no mínimo 32 instâncias de Spanning Tree.

15.7.3. **Deve implementar as seguintes MIBs**

15.7.3.1. Deve implementar RFC 1157 SNMPv1/v2c.

15.7.3.2. Deve implementar RFC 2571 Architecture for Describing SNMP.

15.7.3.3. Deve implementar RFC 2572 SNMP Message Processing and Dispatching.

15.7.3.4. Deve implementar RFC 2573 SNMP Applications.

15.7.3.5. Deve implementar RFC 2576 Coexistence between SNMP versions.

15.8. **ITEM 5 - SWITCH GIGABIT 16 PORTAS**

15.8.1. **Características Gerais**

15.8.1.1. Deve ser fornecido com no mínimo 16 portas 1 GbE RJ-45.

15.8.1.2. Deve ser fornecido com no mínimo 4 slots 1/10 GbE SFP/SFP+.

15.8.1.3. Deve possuir 1 interface RJ-45 ou serial para acesso console local.

15.8.1.4. Deve possuir Certificado de Homologação na Anatel, de acordo com a Resolução nº 242.

15.8.1.5. Deve possuir alimentação interna 110/220VAC 50/60Hz.

15.8.1.6. Deve ser compatível com os itens 1, 2 e 3 deste edital para fins de gerenciamento centralizado.

15.8.1.7. Não serão aceitos equipamentos cujo fabricante tenha anunciado o fim de vendas do modelo (End of Sales).

15.8.2. **Controle**

15.8.2.1. Deve possuir tabela para 32.000 (trinta e dois mil) endereços MAC.

15.8.2.2. Deve possuir capacidade de encaminhamento de no mínimo 190 Mpps.

15.8.2.3. Deve possuir capacidade de comutação de no mínimo 128 Gbps.

15.8.2.4. Deve suportar no mínimo 4.000 VLANs.

15.8.2.5. Deve suportar 8 grupos de agregação de links (padrão IEEE 802.3ad), permitindo até 16 links Gigabit Ethernet por grupo.

15.8.2.6. Deve possuir no mínimo 512 MB de memória RAM.

15.8.2.7. Deve possuir memória flash de no mínimo 64 MB.

15.8.2.8. Deve suportar no mínimo 2 MB de buffer de pacote.

15.8.2.9. Deve suportar no mínimo 640 ACLs.

15.8.2.10. Deve suportar no mínimo 32 instâncias de Spanning Tree.

15.8.3. **Deve implementar as seguintes MIBs**

15.8.3.1. Deve implementar RFC 1157 SNMPv1/v2c.

15.8.3.2. Deve implementar RFC 2571 Architecture for Describing SNMP.

15.8.3.3. Deve implementar RFC 2572 SNMP Message Processing and Dispatching.

15.8.3.4. Deve implementar RFC 2573 SNMP Applications.

15.8.3.5. Deve implementar RFC 2576 Coexistence between SNMP versions.

- 15.9. **ITEM 6 E ITEM 7 - ACCES POINT TIPO 1 E ACCESS POINT TIPO 2**
- 15.9.1. **Exigências mínimas de funcionalidades técnicas**
- 15.9.1.1. Suportar até 8 SSIDs simultâneos.
- 15.9.1.2. Suportar os seguintes tipos de EAP:
- a) EAP-TLS.
 - b) EAP-TTLS/MSCHAPv2.
 - c) PEAPv0/EAP-MSCHAPv2.
 - d) PEAPv1/EAP-GTC.
 - e) EAP-SIM.
 - f) EAP-AKA.
 - g) EAP-FAST.
- 15.9.1.3. Suportar autenticação de usuário/equipamento nas seguintes tecnologias:
- a) WPA.
 - b) WPA2.
 - c) WPA3 com 802.1x ou Preshared key.
 - d) WEP.
 - e) Web Captive Portal.
 - f) MAC blocklist e allowlist.
- 15.9.1.4. Possuir suporte para trava Kensington.
- 15.9.1.5. Possuir os seguintes Padrões IEEE: 6.1.16.1. 802.11a. 6.1.16.2. 802.11b. 6.1.16.3. 802.11be. 6.1.16.4. 802.11e. 6.1.16.5. 802.11g. 6.1.16.6. 802.11h. 6.1.16.7. 802.11i. 6.1.16.8. 802.11j. 6.1.16.9. 802.11k. 6.1.16.10. 802.11n. 6.1.16.11. 802.11r. 6.1.16.12. 802.11v. 6.1.16.13. 802.11ac. 6.1.16.14. 802.11ax. 6.1.16.15. 802.11mc. 6.1.16.16. 802.1X. 6.1.16.17. 802.3af. 6.1.16.18. 802.3at. 6.1.16.19. 802.3bt. 6.1.16.20. 802.3az. 6.1.16.21. 802.1Q. 6.1.16.22. 802.11u. 6.1.16.23. 802.11w. 6.1.16.24. 802.3bz.
- 15.9.1.6. Ter suporte SSID para Local-Bridge, Mesh e Tunnel.
- 15.9.1.7. Possuir capacidade mínima de 512 clientes por rádio.
- 15.9.1.8. Possuir botão de Reset.
- 15.9.1.9. Funcionalidades 802.11:
- a) Suportar OFDMA – Sim (UL and DL).
 - b) Suportar Spatial Reuse (BSS Coloring).
 - c) Suportar Modo UL-MU-MIMO.
 - d) Suportar DL-MU-MIMO.
 - e) Suportar Enhanced Target Wake Time (TWT).
 - f) Suportar ZeroWait DFS.
- 15.9.1.10. Capacidades de monitoramento de wireless:
- a) Suportar Rogue Scan Radio nos modos Background e Dedicado.
 - b) Suportar Radio WIPS/WDS nos modos Background e Dedicado.
 - c) Possuir Modo Sniffer de pacote.
 - d) Possuir analisador de espectro.
- 15.9.1.11. Montagem
- a) Possuir opções de montagem em teto, parede e T-Rail.
 - b) Deve incluir os acessórios necessários para montagem em teto, parede e T-

Rail.

15.9.1.12. Certificações

a) O equipamento ofertado deve possuir certificado Aliança - Wi-Fi.

15.9.1.13. Diversos

a) Gerenciamento via web do ponto de acesso.

b) Deve possuir um painel único de gerenciamento web para total visibilidade e controle de acesso de usuários e equipamentos do mesmo fabricante/modelo na rede, sendo fornecido gratuitamente, e, também, permitir integração para gerenciamento e monitoramento centralizado através do appliance descrito no item 1, bem como ser compatível com os itens 1, 2 e 3 deste edital.

15.10. **ITEM 6 - ACCESS POINT TIPO 1**

15.10.1. **Características Específicas**

15.10.1.1. Deve ser do tipo Ponto de Acesso (AP) para uso interno.

15.10.1.2. Padrão Wi-Fi 6.

15.10.1.3. Possuir, no mínimo, 3 rádios

15.10.1.4. Possuir, no mínimo, 06 antenas Internas

15.10.1.5. Possuir, no mínimo, os seguintes tipos de antena e ganho de pico: PIFA: 4 dBi para 2.4 GHz, 5 dBi para 5 GHz e 5 dBi para 6 GHz.

15.10.1.6. O rádio 1 deve ter as seguintes capacidades mínimas: 2.4 GHz (2x2) 20/40 MHz.

15.10.1.7. O rádio 2 deve ter as seguintes capacidades mínimas: 5.0 GHz (2x2) 20/40/80/160 MHz.

15.10.1.8. O rádio 3 deve ter as seguintes capacidades mínimas: 6.0 GHz (2x2) 20/40/80/160/320MHz.

15.10.1.9. Taxa de dados máxima por rádio:

a) Rádio 1 até 688 Mbps.

b) Rádio 2 até 2882 Mbps.

c) Rádio 3 até 5765 Mbps.

15.10.1.10. Deve possuir as seguintes interfaces:

a) Uma interface 100/1000/2500 Base-T RJ45.

b) Uma interface 1x RS-232 RJ45 Serial Port.

15.11. **ITEM 7 - ACCESS POINT TIPO 2**

15.11.1. **Características Específicas**

15.11.1.1. Deve ser do tipo Ponto de Acesso (AP) para uso interno.

15.11.1.2. Padrão Wi-Fi 6.

15.11.1.3. Possuir, no mínimo, 2 rádios

15.11.1.4. Possuir, no mínimo, 4 antenas Internas

15.11.1.5. Possuir, no mínimo, os seguintes tipos de antena e ganho de pico: PIFA: 4 dBi para 2.4 GHz, 5 dBi para 5 GHz e 5 dBi para 6 GHz.

15.11.1.6. O rádio 1 deve ter as seguintes capacidades mínimas: 2.4 GHz (2x2) 20/40 MHz.

15.11.1.7. O rádio 2 deve ter as seguintes capacidades mínimas: 5.0 GHz (2x2) 20/40/80/160 MHz.

15.11.1.8. Taxa de dados máxima por rádio:

- a) Rádio 1 até 688 Mbps.
- b) Rádio 2 até 2882 Mbps.

15.11.1.9. Deve possuir as seguintes interfaces:

- a) Uma interface 100/1000 Base-T RJ45.
- b) Uma interface 1x RS-232 RJ45 Serial Port.

15.12. **ITEM 8 - SOLUÇÃO DE DETECÇÃO E RESPOSTA ESTENDIDA (XDR)**

15.12.1. **Requisito - licenciamento e instalação**

15.12.1.1. A solução de XDR deve suportar a gestão de, no mínimo, 330 máquinas, simultaneamente.

15.12.1.2. Assinatura válida por 60 (sessenta meses).

15.12.1.3. A solução proposta não deve exigir elementos adicionais na infraestrutura local, com exceção dos agentes (coletores) nas estações e servidores gerenciados.

15.12.2. **Requisito do agente (coletor)**

15.12.2.1. A solução deve ser compatível com os seguintes sistemas operacionais Windows 10 e 11 (versões 32 e 64 bits).

15.12.2.2. A solução deve ser compatível com os seguintes sistemas operacionais Windows Server 2019 e superiores.

15.12.2.3. A solução deve ser compatível com os seguintes sistemas operacionais macOS: OS X v10.10 e superiores.

15.12.2.4. A solução deve ser compatível com os seguintes sistemas operacionais Linux: Ubuntu 18.04 e superiores, Debian 11 e superiores, CentOS 7 e superiores, Red Hat 7.4 e superiores, Fedora 36 e superiores.

15.12.2.5. A solução deve ser capaz de atualizar o terminal sem intervenção do usuário e sem requerer uma reinicialização.

15.12.2.6. A solução deve ter proteção "Anti-violação" no Agente.

15.12.2.7. A solução deve operar sem depender de assinaturas hash locais conhecidas para detecção de arquivos maliciosos.

15.12.2.8. A solução deve ser capaz de registrar em tempo real informações do processo e informações adicionais, como o usuário associado aos eventos.

15.12.2.9. A solução deve permitir a definição de uma senha para desinstalar o agente no terminal.

15.12.2.10. A solução deve ser capaz de gerar um instalador Windows pré-configurado. Essa configuração deve permitir a instalação sem necessidade de interação ou configuração do usuário.

15.12.2.11. O coletor deve ser capaz de funcionar em ambientes com proxy.

15.12.2.12. A solução deve ser capaz de operar plenamente com o requerimento mínimo de 400MB de memória RAM; e 1,2GB de espaço em disco, nos sistemas operacionais Windows, Linux e MacOS, com exceção dos servidores;

15.12.2.13. Deve possuir integração nativa com as soluções de Firewall, Sandbox, proteção de Email, controle de acesso (NAC), orquestração de eventos (SOAR) e agregação de logs (SIEM), do mesmo fabricante;

15.12.2.14. A solução deve ser capaz de atualizar automaticamente uma lista dinâmica de endereços de IP no Firewall, relacionados a evento de segurança;

15.12.3. **Requisito - detecção de malware**

15.12.3.1. A solução deve ser capaz de operar no modo "offline", mesmo quando o Agente não estiver conectado à rede corporativa.

15.12.3.2. A solução deve ser capaz de detectar processos em execução, inícios e paradas de processos, e interações entre processos.

15.12.3.3. A solução deve ser capaz de detectar, remover e restaurar ao seu estado original as modificações feitas por processos maliciosos no registro do PC.

15.12.3.4. A solução deve ser capaz de detectar as solicitações de DNS originadas do dispositivo.

15.12.3.5. A solução deve ser capaz de detectar conexões de rede a partir do dispositivo.

15.12.3.6. A solução deve ser capaz de detectar atividades suspeitas relacionadas a arquivos DLL.

15.12.3.7. A solução deve ser capaz de incorporar inteligência de ameaças ao seu esquema de detecção.

15.12.3.8. A solução deve ser capaz de incorporar as técnicas MITRE ATT&CK no esquema de detecção e apresentar quais técnicas foram utilizadas.

15.12.3.9. A solução deve ter a capacidade de procurar ameaças nas estações Windows usando indicadores de comprometimento (IOC), como: nome e hash do arquivo, etc.

15.12.3.10. A solução deve ter a capacidade de procurar ameaças usando IOCs, como ações relacionadas a arquivos (Criação, Exclusão, Renomear).

15.12.3.11. A solução deve ter a capacidade de procurar ameaças usando IOCs, como ações relacionadas a processos (Terminação de Processo, Criação de Processo, Carregamento de Executáveis).

15.12.3.12. A solução deve ter a capacidade de procurar ameaças usando IOCs, como ações relacionadas ao uso da rede (Socket Connect, Socket Close, Socket Bind).

15.12.3.13. A solução deve ter a capacidade de procurar ameaças usando IOCs, como ações relacionadas aos logs do Windows (Log de eventos).

15.12.3.14. A solução deve ter a capacidade de procurar ameaças usando IOCs, como ações relacionadas ao registro do Windows (criação de chave, exclusão de chave, conjunto de valores).

15.12.3.15. A solução deve ter a capacidade de realizar consultas de texto livre para refinar as informações disponíveis na caça de ameaças.

15.12.3.16. A solução deve ter a capacidade de salvar pesquisas realizadas para uso futuro.

15.12.3.17. A solução deve ter a capacidade de agendar a execução de pesquisas salvas.

15.12.3.18. A solução deve identificar atividades maliciosas conhecidas.

15.12.3.19. A solução deve ter a capacidade de receber atualizações diárias de inteligência.

15.12.3.20. A solução deve ter a capacidade de classificar os eventos detectados em diferentes categorias (Ex: Malicioso, Suspeito, Inconclusivo, Provavelmente Seguro).

15.12.3.21. A solução deve ser capaz de coexistir com outras soluções de segurança de endpoint (antivírus tradicional ou de nova geração).

15.12.4. **Requisito - Prevenção de malware**

15.12.4.1. A solução deve ter a capacidade de prevenir a execução de arquivos maliciosos.

15.12.4.2. A solução deve incluir um mecanismo de antivírus de última geração (Next-Generation Antivírus) baseado no kernel do sistema operacional, com capacidade de "Aprendizado de Máquina" (Machine Learning).

15.12.4.3. A solução deve ter a capacidade de controlar dispositivos USB.

15.12.4.4. A solução deve ter a capacidade de criar exceções para dispositivos USB com base no nome do dispositivo.

15.12.4.5. A solução deve ter a capacidade de criar exceções para dispositivos USB com base no fornecedor.

15.12.4.6. A solução deve ter a capacidade de criar exceções para dispositivos USB com

base em uma combinação de: nome do dispositivo, fornecedor, número de série.

15.12.4.7. A solução deve ser capaz de bloquear o tráfego malicioso de exfiltração de dados.

15.12.4.8. A solução deve ser capaz de bloquear o tráfego de comunicação malicioso para C&C (Comando e Controle).

15.12.4.9. A solução deve ser capaz de impedir violações de segurança e tentativas de ransomware em tempo real.

15.12.4.10. A solução deve ser capaz de evitar a criptografia causada por ransomware e modificação de arquivos ou registro. Caso ocorra, a solução deverá restaurar os arquivos afetados/modificados ao seu estado original em tempo real.

15.12.4.11. A solução deve permitir a modificação das políticas, com vários estados, como: ativado, desativado ou apenas gerar "logs" para as regras de segurança.

15.12.4.12. A solução deve ser capaz de ser configurada em modo de simulação, onde não há bloqueio, mas todas as atividades maliciosas são registradas.

15.12.4.13. A solução deve permitir a modificação das regras de detecção de eventos maliciosos para que essas regras apenas armazenem um registro ou operem em modo de bloqueio.

15.12.4.14. A solução deve permitir verificações periódicas dos arquivos nos dispositivos com o Agente instalado.

15.12.5. **Requisito - difusão (pós-infecção)**

15.12.5.1. A solução deve permitir o isolamento automático do tráfego de rede de um dispositivo onde foi detectada atividade de malware.

15.12.5.2. A solução deve permitir alterar as políticas atribuídas a um dispositivo onde foi detectada atividade de malware.

15.12.5.3. A solução deve permitir o bloqueio de atividades realizadas por arquivos maliciosos.

15.12.5.4. A solução deve ter a capacidade de criar exceções para processos com base na localização do arquivo (Caminho do Arquivo).

15.12.5.5. A solução deve ter a capacidade de criar exceções para processos com base no destino do tráfego gerado pelo processo.

15.12.5.6. A solução deve ter a capacidade de criar exceções para os processos baseados no usuário que o executou.

15.12.5.7. A solução deve ter a capacidade de criar exceções manualmente para falsos positivos, marcando a atividade para evitar falhas futuras.

15.12.5.8. A solução deve ter a capacidade de reclassificar automaticamente a atividade como um falso positivo para evitar detecções semelhantes.

15.12.5.9. A solução deve permitir a criação de exceções de eventos com base em endereços IP, aplicações e protocolos.

15.12.6. **Requisito - resposta ao incidente**

15.12.6.1. A solução deve permitir o armazenamento de histórico dos eventos.

15.12.6.2. A solução deve armazenar metadados gerados pelos dispositivos, que podem ser usados em investigações forenses.

15.12.6.3. A solução deve permitir a integração com plataformas SIEMs (Security Information and Event Management) através de syslog.

15.12.6.4. A solução deve ser capaz de obter instantâneos de memória ou "dumps" de memória para possibilitar processos forenses.

15.12.6.5. A solução deve ser capaz de abrir tickets em plataformas de gerenciamento como ServiceNow e JIRA.

15.12.6.6. A solução deve permitir a integração via API, fornecendo informações geradas em um evento (como endereço IP, nome do host, usuário, data/hora, atividade suspeita, etc.).

15.12.6.7. A solução deve ter a capacidade de encerrar um processo com base em sua classificação.

15.12.6.8. A solução deve ter a capacidade de excluir um arquivo com base em sua classificação.

15.12.6.9. A solução deve ter a capacidade de restaurar as configurações de registro básicas com base na classificação de atividade predefinida.

15.12.6.10. A solução deve ter a capacidade de isolar os dispositivos infectados da rede.

15.12.6.11. A solução deve ter a capacidade de restringir automaticamente o acesso do dispositivo à rede de acordo com a classificação (Malicioso, Suspeito, etc.) do processo detectado.

15.12.6.12. A solução deve obter visibilidade completa da cadeia de ataques e alterações maliciosas.

15.12.6.13. A solução deve permitir a limpeza automática do dispositivo e a reversão de alterações maliciosas, mantendo o dispositivo operacional.

15.12.6.14. A solução deve permitir a assinatura de serviços opcionais de detecção e resposta a incidentes (Ex: serviços gerenciados de detecção e resposta).

15.12.6.15. A solução deve permitir o envio de executáveis para análise em um sandbox, a fim de determinar se são maliciosos ou inofensivos.

15.12.6.16. A solução deve possuir integração com Active Directory para viabilizar o uso de playbooks para contenção e resposta a incidentes de segurança.

15.12.6.17. A solução deve fornecer mecanismos de proteção diversificados, incluindo o encerramento de um processo, a exclusão de um arquivo malicioso e o bloqueio de uma conexão de rede.

15.12.7. **Requisito - controle de vulnerabilidade e comunicação**

15.12.7.1. A solução deve ser capaz de descobrir aplicativos que se comunicam pela rede e que apresentam risco para o terminal.

15.12.7.2. A solução deve ser capaz de realizar um patch virtual, através da restrição de acessos de comunicação nas aplicações vulneráveis.

15.12.7.3. A solução deve permitir a diminuição das superfícies de ataque por meio de políticas de comunicação proativas baseadas no risco (de acordo com o CVE e a qualificação/reputação da aplicação).

15.12.7.4. A solução deve ser capaz de impedir que aplicativos não autorizados se comuniquem pela rede.

15.12.7.5. A solução deve ser capaz de criar políticas que bloqueiem a comunicação de aplicativos com base na versão instalada.

15.12.7.6. A solução deve ser capaz de detectar e identificar todas as aplicações nos dispositivos que se comunicam na rede.

15.12.7.7. A solução deve ser capaz de fornecer informações sobre o uso de aplicativos de rede, mostrando, por exemplo, quais dispositivos geram tráfego para um aplicativo.

15.12.7.8. A solução deve ser capaz de visualizar e fornecer informações sobre o uso dos aplicativos de rede, como os destinos IP do tráfego gerado.

15.12.8. **Requisito - cenários de ataque**

15.12.8.1. A solução deve identificar e prevenir tentativas de escalonamento de privilégios.

15.12.8.2. A solução deve bloquear ataques de ransomware conhecidos.

15.12.8.3. A solução deve detectar malware desconhecido como RAT (Trojan de acesso remoto) através das atividades do malware, e não por assinatura.

15.12.8.4. A solução deve proteger contra scripts Powershell maliciosos.

15.12.8.5. A solução deve proteger contra scripts CScript maliciosos.

15.12.8.6. A solução deve proteger contra macros maliciosas do Office.

15.12.8.7. A solução deve ter controle sobre dispositivos USB.

15.12.9. **Requisito - Detecção e Resposta Estendida**

15.12.9.1. A solução deve suportar detecção estendida de anomalias ou atividades maliciosas, originadas de eventos de múltiplos sistemas de segurança.

15.12.9.2. A solução deve suportar a detecção de, no mínimo, as seguintes anomalias ou atividades maliciosas:

a) Varredura de rede e portas.

b) Tentativas de acesso por força bruta.

c) Atividades de Comando e Controle (C2C).

d) Phishing.

e) Movimentação lateral.

f) Exfiltração de dados.

g) Comprometimento de credenciais e contas.

h) ARP spoofing.

15.12.9.3. Para eventos coletados em sistemas de terceiros, a solução deve aplicar análises e correlação de dados assistidos por IA (inteligência artificial).

15.12.9.4. A solução deve permitir que anomalias ou atividades maliciosas, detectadas em soluções de segurança de terceiros, sejam classificadas como violações de segurança.

15.12.9.5. A solução deve possuir, de forma nativa, conector para com o AWS Guard Duty.

15.12.9.6. A partir de anomalias ou atividades maliciosas detectadas em sistemas de terceiros, a solução deve ser capaz de disparar automações em soluções de segurança e infraestrutura, como firewalls, NACs, segurança de e-mail e identidade.

15.12.10. **Requisito IOT**

15.12.10.1. A solução deve ser capaz de descobrir dispositivos IOT não gerenciados na rede.

15.12.10.2. A solução deve ser capaz de detectar dispositivos não gerenciados e protegidos com sistemas operacionais macOS / Linux / Windows.

15.12.11. **Requisito - console de administração**

15.12.11.1. A Solução deve incluir políticas de segurança e playbooks básicos pré-definidos, eliminando a necessidade de criação manual após a instalação.

15.12.11.2. Se oferecida em nuvem, a solução deve estar em conformidade com o padrão da AICPA SOC.

15.12.11.3. A solução deve estar em conformidade com o padrão GDPR.

15.12.11.4. O console de gerenciamento deve permitir a integração com o "Active Directory" para garantir o cumprimento da política de senhas da empresa.

15.12.11.5. O console de administração deve permitir o uso de autenticação de dois fatores (2FA) para acesso.

15.12.11.6. O console de administração deve permitir a integração com SAML para autenticação do usuário.

15.12.11.7. O console de administração deve permitir o uso de funções granulares para administradores.

15.12.11.8. O console de administração deve permitir o gerenciamento de ambientes multi-inquilinos (multilocatários).

15.12.11.9. O console de administração deve permitir o gerenciamento por meio da API Full

Restful.

15.12.11.10A solução deve ser capaz de ser inteiramente gerenciada na nuvem do fabricante ou pelo appliance do item 1.

15.12.11.11A solução deve possuir integração nativa com soluções de controle de acesso.

15.12.11.12A solução deve possuir integração nativa com soluções de SIEM.

15.12.11.13A solução deve possuir integração nativa com soluções de firewall.

15.12.11.14A solução deve possuir integração nativa com soluções Sandbox.

15.12.11.15A solução deve suportar integração com a base de dados do fabricante para atualizações de inteligência de ameaças contra malwares.

15.12.11.16O console de administração deve permitir a visualização dos eventos registrados nos dispositivos que necessitam de atenção.

15.12.11.17O console de administração deve permitir a visualização da saúde dos Agentes instalados.

15.12.11.18O console de administração deve permitir a desinstalação remota do Agente nos dispositivos.

15.12.11.19O console de administração deve permitir a desativação / ativação remota do Agente.

15.12.11.20O console de administração deve permitir a atualização remota do Agente.

15.12.11.21O console de administração deve permitir a criação de relatórios executivos com um resumo dos eventos de segurança e o status do sistema.

15.12.11.22O console de administração deve permitir a criação de grupos organizacionais de dispositivos, onde cada grupo pode ter regras de proteção independentes.

15.12.11.23O console de administração deve permitir a exportação dos logs locais gerados pelos Agentes.

15.12.11.24O console de administração deve permitir a criação de relatórios de inventário dos Agentes implantados, incluindo: Endereço IP, Nome do Host, Sistema Operacional, Endereço MAC, Versão do Agente instalado, Status do Agente e Último dia visto pelo console.

15.12.11.25O console de gerenciamento deve ter visibilidade dos eventos gerados pelos dispositivos ou eventos conforme o processo executado.

15.12.11.26O console de administração deve permitir a integração de um SMTP externo para o envio de alertas por e-mail.

15.12.11.27O console de administração deve permitir auditorias de alterações feitas por administradores/operadores. Essas auditorias também devem poder ser baixadas em formato CSV.

15.12.11.28A solução deve permitir o isolamento de um dispositivo através da integração de um NAC (Network Access Control) conforme a categoria do evento detectado.

15.12.11.29A solução deve permitir adicionar endereços IP maliciosos detectados em um ou mais firewalls remotos integrados.

15.12.11.30A solução deve permitir a configuração de perfis nas informações coletadas para a caça a ameaças.

15.12.11.31A solução deve permitir exclusões de informações que não serão coletadas na função de caça a ameaças.

15.12.11.32A solução deve entregar informações geradas pelos serviços de inteligência para auxiliar na tomada de decisão na nuvem sobre o evento detectado.

15.12.11.33A solução deve permitir que os serviços em nuvem recategorizem uma classificação de evento.

15.12.11.34A solução deve permitir que os administradores desabilitem as notificações para

um evento de descoberta.

15.12.12. Requisitos técnicos gerais

15.12.12.1. Deve permitir o gerenciamento remoto dos clientes de segurança, a partir de um console central do próprio fabricante.

15.12.12.2. O licenciamento deve se basear no número de clientes registrados no console de gerenciamento central do mesmo fabricante.

15.12.12.3. Deve ser compatível com, pelo menos, os seguintes sistemas operacionais Microsoft Windows: 10 (32 e 64 bits) e 11(64 bits); Microsoft Windows Server: 2019 e superiores; Mac OS X: v10.10 e superiores; Linux: Ubuntu 18.04 e superiores, Debian 11 e superiores, CentOS 7 e superiores, Red Hat 7.4 e superiores, Fedora 36 e superiores.

15.12.12.4. Deve ter uma interface gráfica do usuário em, pelo menos, nos idiomas inglês e português.

15.12.12.5. Deve permitir o backup do arquivo de configuração.

15.12.12.6. Deve ser capaz de gerar um registro de eventos (logs) nas funcionalidades instaladas e configuradas.

15.12.12.7. Deve suportar pelo menos os seguintes níveis de log: emergência, alerta, crítico, erro, aviso, informativo.

15.12.12.8. Os clientes de segurança devem poder enviar os logs para o servidor console de gerenciamento central.

15.12.12.9. O cliente de segurança deve suportar integração às tecnologias Sandboxing, pelo menos do mesmo fabricante.

15.12.12.10 Deve controlar o acesso a dispositivos removíveis e ser capaz de monitorar, permitir ou negar acesso a dispositivos USB.

15.12.12.11 Deve poder definir o nível do log: emergência, alerta, crítico, erro, aviso, depuração, informações.

15.12.12.12 Deve ter um agente de logon único.

15.12.12.13 Deve ter a capacidade de desabilitar os serviços de proxy para erros de depuração.

15.12.12.14 Deve ser capaz de ativar seletivamente logs em: VPN, Antivírus, Atualizações, Sandboxing, Comunicação com segurança cooperativa, filtro de web e verificação de vulnerabilidade.

15.12.12.15 Deve suportar a exportação dos logs para fora do cliente de segurança.

15.12.12.16 Deve ser capaz de integrar-se a uma estrutura cooperativa para compartilhamento de informações e recebimento de atualizações de assinaturas dinâmicas.

15.12.12.17 Deve ser capaz de enviar informações como: usuário conectado, inventário de software, processos, versão do sistema operacional e estado do antivírus (data da base de assinatura e se está em execução) para uso na análise de conformidade do dispositivo.

15.12.12.18 Deve suportar o envio de logs para um analisador central de logs, onde os índices de comprometimento do cliente (IoC) são processados (taxas de confirmação).

15.12.12.19 Deve suportar o recebimento de atualizações de assinaturas dinâmicas da solução de proteção avançada de ameaças (ATP) ou Sandboxing.

15.12.12.20 Deve ser disponibilizada uma ferramenta que permita a aplicação de políticas distintas, independentemente de o cliente estar conectado à rede corporativa.

15.12.12.21 Deve permitir que o cliente fique em quarentena no console central ou em outro componente da solução de segurança cooperativa.

15.12.13. Funcionalidade de anti-malware

15.12.13.1. O cliente de segurança deve ter a capacidade de inspecionar arquivos executáveis, bibliotecas e drivers em busca de vírus.

15.12.13.2. O cliente de segurança deve ser capaz de verificar automaticamente as atualizações de assinatura.

15.12.13.3. O cliente de segurança deve ser capaz de enviar arquivos para inspeção nos sistemas Sandboxing do mesmo fabricante.

15.12.13.4. O cliente de segurança deve ser capaz de bloquear os canais de comunicação utilizados por hackers ou atacantes.

15.12.13.5. O cliente de segurança deve notificar localmente quando um vírus é detectado.

15.12.13.6. O cliente de segurança deve permitir que o usuário inicie uma verificação sob demanda.

15.12.13.7. O cliente de segurança deve permitir que a verificação de vírus seja iniciada automaticamente em intervalos regulares.

15.12.13.8. O cliente de segurança deve permitir a visualização dos arquivos em quarentena.

15.12.13.9. Deve permitir a configuração do perfil antivírus a partir do console central do mesmo fabricante.

15.12.13.10 Deve ter uma solução de proteção contra malware baseada em nuvem. Essa proteção deve ser capaz de gerar uma soma de verificação (checksum) do arquivo acessado e consultar a nuvem se essa soma corresponde a uma nova ameaça.

15.12.13.11 A ferramenta de proteção baseada em nuvem NÃO deve enviar o arquivo inteiro ou seus metadados, mas SOMENTE a soma de verificação.

15.12.13.12 A ferramenta de proteção baseada em nuvem deve analisar apenas arquivos de alto risco, como (entre outros) documentos do Word, Excel, PDF e DLL.

15.12.13.13 Deve ter uma solução de Anti-Exploit, que protege o endpoint de ameaças em tempo real, monitorando o comportamento de aplicativos populares, incluindo leitores do Office, Internet Explorer, Chrome, Firefox, Java, Flash e PDF, etc.

15.12.13.14 Deve ser capaz de proteger arquivos, tipos de arquivos específicos ou pastas contra alterações não autorizadas.

15.12.13.15 Caso seja detectado um comportamento de criptografia não autorizada (Ransomware), a solução deve ser capaz de restaurar o arquivo ou pasta.

15.12.13.16 Deve ser capaz de enviar arquivos para uma solução de proteção avançada de ameaças (ATP) (ou sandboxing) antes de serem acessados.

15.12.13.17 Deve suportar sandbox localmente ou através de uma solução em nuvem.

15.12.13.18 Deve ser capaz de bloquear o acesso ao arquivo até que o sandbox forneça um veredicto.

15.12.13.19 Caso um arquivo seja classificado como malicioso pela Sandbox, deve ser mantido em quarentena.

15.12.14. Funcionalidade de Firewall de Aplicação

15.12.14.1. O cliente de segurança deve suportar perfis de Controle de Aplicativos, criados de forma centralizada no console de gerenciamento do mesmo fabricante.

15.12.14.2. O fabricante deve permitir que os clientes de segurança realizem consultas on-line sobre a categoria de um aplicativo para ser usada na política de controle de acesso.

15.12.14.3. Deve possuir pelo menos 4000 aplicativos reconhecidos em sua base para uso nas regras de controle de acesso dos clientes de segurança.

15.12.15. Funcionalidade de Filtro Web

15.12.15.1. Deve permitir a configuração do perfil de filtro da web a partir do console central do mesmo fabricante.

15.12.15.2. O fabricante deve fazer consultas on-line com o cliente de segurança sobre a categoria de um site (por exemplo, interesse geral, tecnologia, hackers, pornografia etc.) para aplicar a política de controle de acesso à Internet.

15.12.15.3. O cliente de segurança deve suportar regras estáticas de acesso à Internet baseadas em expressões regulares.

15.12.15.4. Para uma URL específica, os acessos devem ter as ações: permitir, bloquear, alertar ou monitorar.

15.12.15.5. Deve configurar o filtro de URL fornecido pelo fabricante com pelo menos as seguintes ações: bloquear, avisar, permitir e monitorar.

15.12.15.6. Deve configurar o filtro de URL com base em caracteres curingas (wildcards) ou expressões regulares (regex) com as seguintes ações: bloquear ou permitir.

15.12.16. Funcionalidades de Análise de Vulnerabilidade

15.12.16.1. O cliente de segurança deve ter um módulo de pesquisa de vulnerabilidades integrado e permitir o gerenciamento central no console do mesmo fabricante.

15.12.16.2. Deve permitir que o usuário inicie uma análise de vulnerabilidade sob demanda.

15.12.16.3. As vulnerabilidades detectadas devem ser exibidas localmente com um link para visualizar informações de um banco de dados na Internet. Deve incluir pelo menos: nome, gravidade e detalhes.

15.12.16.4. Os resultados da verificação de vulnerabilidades devem incluir, no mínimo: lista de vulnerabilidades e o número de vulnerabilidades classificadas como críticas, altas, médias e baixas.

15.12.16.5. Devem ser fornecidos links de acesso a informações complementares, como links para a página do fabricante detalhando as características da vulnerabilidade.

15.12.16.6. Deve permitir a aplicação automática de patches.

15.12.16.7. Deve detalhar quais correções exigem instalação manual.

15.12.16.8. A verificação de vulnerabilidades deve ser permitida de maneira sequencial e autônoma a partir do console central.

15.12.16.9. Deve verificar as vulnerabilidades antes da aplicação de patches.

15.12.17. Funcionalidade de clientes VPN

15.12.17.1. IPSEC VPN.

15.12.17.2. Deve permitir que o usuário crie novas VPNs IPSEC.

15.12.17.3. Deve permitir que múltiplas VPNs IPSEC sejam definidas simultaneamente.

15.12.17.4. Deve permitir a autenticação usando nome de usuário e senha.

15.12.17.5. Deve permitir a autenticação usando certificados digitais.

15.12.17.6. Deve permitir a seleção dos modos Principal e Agressivo.

15.12.17.7. Deve permitir a configuração do DHCP por IPSec.

15.12.17.8. Deve permitir o uso do NAT Traversal.

15.12.17.9. Deve permitir a escolha de grupos Diffie-Hellman (1, 2, 5 e 14).

15.12.17.10 Deve permitir configurações de expiração de chave IKE.

15.12.17.11 Deve suportar IKEv1 e IKEv2.

15.12.17.12 Deve permitir o uso do Perfect Forward Secrecy.

15.12.17.13 Deve permitir a autenticação de dois fatores fornecida pelo mesmo fabricante.

15.12.17.14 Deve permitir a configuração de túneis divididos (Split tunnel), separando o tráfego entre acesso à Internet e uso de VPN.

15.12.18. Funcionalidade de Gerenciamento Centralizado

15.12.18.1. Deve permitir a instalação on-premises no Microsoft Windows Server 2019 e superiores.

15.12.18.2. O console de gerenciamento centralizado deve ser entregue sem custo.

- 15.12.18.3. Deve permitir a adição de clientes através da adição de licenças.
- 15.12.18.4. Deve ter interface gráfica de gerenciamento.
- 15.12.18.5. Deve comunicar-se com os endpoints por meio de um canal criptografado TLS 1.3.
- 15.12.18.6. Deve permitir a criação de usuários com diferentes perfis administrativos.
- 15.12.18.7. Deve permitir a importação de informações do Active Directory usando LDAP.
- 15.12.18.8. Deve permitir o registro manual da estação através de uma senha.
- 15.12.18.9. Deve permitir a criação de grupos de clientes para facilitar a gestão.
- 15.12.18.10 Deve permitir a configuração do cliente através de definições em XML.
- 15.12.18.11 Deve permitir que as configurações de perfil sejam importadas em um dispositivo de firewall do mesmo fabricante.
- 15.12.18.12 Deve permitir a configuração de diferentes grupos e perfis para facilitar a administração.
- 15.12.18.13 Deve permitir a configuração de antivírus, filtro da web, controle de aplicativos, verificador de vulnerabilidades e perfis de VPN.
- 15.12.18.14 Deve permitir a proteção em tempo real
- 15.12.18.15 Deve permitir a configuração de varreduras de vírus e vulnerabilidades agendadas.
- 15.12.18.16 Deve permitir verificação completa e verificação rápida.
- 15.12.18.17 Deve permitir que o usuário configure VPNs localmente.
- 15.12.18.18 Deve permitir que o usuário desconecte uma VPN.
- 15.12.18.19 Deve permitir a conexão VPN antes do login.
- 15.12.18.20 Deve permitir conexão VPN automática.
- 15.12.18.21 Deve suportar o uso específico ou geral para VPN IPSec (pelo menos).
- 15.12.18.22 Deve suportar o uso de certificados ou usuário e senha para autenticação.
- 15.12.18.23 Deve suportar o uso de certificados no cartão inteligente.
- 15.12.18.24 Deve suportar o bloqueio de tráfego IPv6.
- 15.12.18.25 Deve suportar a opção para o usuário acessar a configuração do cliente por senha.
- 15.12.18.26 Deve ser capaz de enviar logs para um sistemas de log externo.
- 15.12.18.27 Deve permitir a instalação do certificado digital no cliente.
- 15.12.18.28 Deve permitir ativar as funcionalidades de Logon Único (Single Sign-On).
- 15.12.18.29 Deve ter informações disponíveis sobre: Número de dispositivos gerenciados, Versão do sistema operacional, Perfil aplicado, Usuário, Versão de assinatura do antivírus, Status do cliente de segurança (Registrado ou não registrado).
- 15.12.18.30 Deve conter informações sobre o sistema operacional no qual o cliente está instalado.
- 15.12.18.31 Deve informar o perfil de segurança criado e / ou aplicado.
- 15.12.18.32 Deve informar os recursos de segurança aplicados: antivírus, filtro da web, VPN, firewall de aplicativo.
- 15.12.18.33 Deve permitir habilitar ou desabilitar os recursos antivírus, filtro da web, VPN, firewall de aplicativo nos terminais gerenciados.
- 15.12.18.34 Deve ser capaz de realizar um inventário do software instalado em cada nó de extremidade.
- 15.12.18.35 Deve permitir a implantação automática de clientes de terminal de acordo com a OU do MS AD ou grupos do MS AD.

15.12.18.36 Deve permitir a manutenção de múltiplas instâncias de instaladores com diferentes recursos (AV, VPN, WF, etc.) e arquiteturas (x86, x64, etc.).

15.12.18.37 Deve permitir a implantação em equipamentos que NÃO pertencem ao Active Directory (AD).

15.12.18.38 Deve permitir a criação de regras de conformidade que avaliem a postura do dispositivo e ajudem o administrador a controlar o acesso, impedindo que um cliente não conforme se conecte a redes críticas.

15.12.18.39 Deve ser capaz de ser acessado através da administração WEB.

15.12.18.40 Deve ter um painel para verificação rápida do status de integridade dos clientes.

15.12.18.41 Deve gerenciar listas centralizadas de quarentena de arquivos.

15.12.18.42 Deve permitir aplicar políticas aos terminais de acordo com os grupos, garantindo que todos os clientes do grupo tenham a mesma política.

15.12.18.43 Deve poder atribuir configurações dinamicamente quando os clientes mudam de grupo.

15.12.18.44 As políticas de terminal devem atribuir perfis de proteção aos terminais. Esses perfis devem ser uma forma de implantar uma configuração exclusiva de: malware, sandboxing, webfilter, firewall de aplicativos, VPN, verificação de vulnerabilidades e configurações do sistema logfiles).

15.12.18.45 Os usuários administradores devem poder sincronizar com o AD para permitir o login com as mesmas credenciais.

15.12.18.46 Deve ser capaz de definir funções administrativas.

15.12.18.47 Deve suportar o backup / restauração das configurações do console, configuração do servidor e políticas de terminal.

15.12.19. **Visibilidade**

15.12.19.1. Deve suportar o upload de uma foto ou avatar para identificação rápida do usuário.

15.12.19.2. Deve relatar rapidamente o nível de vulnerabilidade da estação de trabalho.

15.12.19.3. Deve ter um sistema de notificação pop-up.

15.12.19.4. Deve ter uma lista de notificações atuais e passadas.

15.12.19.5. As notificações devem incluir: eventos AV, eventos ATP, eventos de comunicação, eventos de filtro da web e eventos do sistema.

15.12.19.6. Deve fornecer informações sobre a vulnerabilidade, patches, versões afetadas, etc., bem como o CVE correspondente.

15.12.19.7. Deve fornecer uma lista de aplicativos bloqueados.

15.12.19.8. Caso o cliente seja colocado em quarentena, deverá ser capaz de informar ao usuário e notificar o gerenciamento.

15.12.19.9. Deve suportar a exibição de uma lista de explorações detectadas.

15.12.19.10 Deve permitir exibir uma lista de aplicativos protegidos contra exploração.

15.12.19.11 Deve fornecer uma lista de arquivos em quarentena.

15.12.19.12 Deve ser possível visualizar os resultados da análise ATP.

15.12.19.13 O fabricante deve fornecer um portal para download da segurança do cliente e permitir a instalação local.

15.12.19.14 Deve ser compatível com a instalação via Microsoft Active Directory.

15.12.19.15 O console de gerenciamento central deve ser capaz de instalar o cliente de segurança nos computadores Windows associados a um domínio da Microsoft.

15.12.19.16 Deve ser capaz de enviar e-mails de convite aos usuários do endpoint, auxiliando

na conexão ao serviço de gerenciamento centralizado.

15.13. ITEM 9 - LICENCIAMENTO, ATUALIZAÇÕES, SUPORTE (24X7) PELO FABRICANTE E GARANTIA DE 60 MESES DE TODOS OS PRODUTOS DA SOLUÇÃO

15.13.1. Características de licenciamento e suporte do fabricante para o item 1

15.13.1.1. Suporte técnico do fabricante na modalidade 24 horas por dia, 7 dias por semana (24x7h) durante 60 meses.

15.13.1.2. O tempo de resposta para problemas críticos não deve exceder 1 hora.

15.13.1.3. Os chamados devem ser abertos através de portal WEB e telefone 0800, sendo possível solicitar atendimento em língua portuguesa.

15.13.1.4. Deve possuir portal web para abertura de chamados.

15.13.1.5. O up-grade de firmware deve ser garantido durante o período de garantia e suporte.

15.13.2. Características de licenciamento e suporte do fabricante para o item 2

15.13.2.1. Suporte técnico do fabricante na modalidade 24x7h durante 60 meses.

15.13.2.2. O tempo de resposta para problemas críticos deve ser de até 1 hora.

15.13.2.3. Os chamados devem ser abertos através de portal WEB e telefone 0800, com a opção de atendimento em língua portuguesa.

15.13.2.4. Deve possuir portal web para abertura de chamados.

15.13.2.5. O up-grade de firmware deve ser garantido durante o período de garantia e suporte.

15.13.2.6. As funcionalidades de controle de aplicação, IPS, gateway anti-malware, filtro de conteúdo web, filtro de DNS e o suporte deverão estar licenciadas por 60 meses.

15.13.3. Características de licenciamento e suporte do fabricante para o item 3

15.13.3.1. Suporte técnico do fabricante na modalidade 24x7h durante 60 meses.

15.13.3.2. O tempo de resposta para problemas críticos deve ser de até 1 hora.

15.13.3.3. Os chamados devem ser abertos através de portal WEB e telefone 0800, com a opção de atendimento em língua portuguesa.

15.13.3.4. Deve possuir portal web para abertura de chamados.

15.13.3.5. O up-grade de firmware deve ser garantido durante o período de garantia e suporte.

15.13.3.6. As funcionalidades de controle de aplicação, IPS, gateway anti-malware, filtro de conteúdo web, filtro de DNS e o suporte deverão estar licenciadas por 60 meses.

15.13.4. Características de licenciamento e suporte do fabricante para o item 4

15.13.4.1. Suporte técnico do fabricante na modalidade 24x7h durante 60 meses.

15.13.4.2. O tempo de resposta para problemas críticos deve ser de até 1 hora.

15.13.4.3. Os chamados devem ser abertos através de portal WEB e telefone 0800, com a opção de atendimento em língua portuguesa.

15.13.4.4. Deve possuir portal web para abertura de chamados.

15.13.4.5. O up-grade de firmware deve ser garantido durante o período de garantia e suporte.

15.13.5. Características de licenciamento e suporte do fabricante para o item 5

15.13.5.1. Suporte técnico do fabricante na modalidade 24x7h durante 60 meses.

15.13.5.2. O tempo de resposta para problemas críticos deve ser de até 1 hora.

- 15.13.5.3. Os chamados devem ser abertos através de portal WEB e telefone 0800, com a opção de atendimento em língua portuguesa.
- 15.13.5.4. Deve possuir portal web para abertura de chamados.
- 15.13.5.5. O up-grade de firmware deve ser garantido durante o período de garantia e suporte.
- 15.13.6. **Características de licenciamento e suporte do fabricante para o item 6**
- 15.13.7. Suporte técnico do fabricante na modalidade 24x7h durante 60 meses.
- 15.13.8. O tempo de resposta para problemas críticos deve ser de até 1 hora.
- 15.13.9. Os chamados devem ser abertos através de portal WEB e telefone 0800, com a opção de atendimento em língua portuguesa.
- 15.13.10. Deve possuir portal web para abertura de chamados.
- 15.13.11. O up-grade de firmware deve ser garantido durante o período de garantia e suporte.

15.14. **ITEM 10 - SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO**

15.14.1. **Serviços de instalação e configuração**

15.14.1.1. A configuração lógica pode ser executada remotamente, desde que a instalação física seja realizada presencialmente.

15.14.1.2. Configuração do Appliance de gerenciamento centralizado (item 1):

- a) Configurações básicas de conectividade.
- b) Registro e ativação de licenças e Atualização de software.
- c) Configuração de Dashboard.
- d) Integração com os equipamentos a serem gerenciados.
- e) Testes de funcionalidade.

15.14.2. **Configuração de firewall (itens 2 e 3)**

15.14.2.1. Configurações básicas de conectividade.

15.14.2.2. Importação/ reprodução fac símile das regras, VLANs, VPNs existentes na infraestrutura atual

15.14.2.3. Registro e ativação de licenças e Atualização de software.

15.14.2.4. Configuração de zonas de segurança, VLANs e roteamento interno.

15.14.2.5. Configurações dos serviços de segurança como IPS e Anti-Malware.

15.14.2.6. Configuração de balanceamento de carga de links WAN.

15.14.2.7. Migração e/ou configuração de regras de firewall.

15.14.2.8. Configuração de VPN.

15.14.2.9. Configuração de regras de aplicação.

15.14.2.10. Integração com base LDAP ou Radius.

15.14.2.11. Configuração de autenticação SSO (Single Sign-On).

15.14.2.12. Configuração de filtro de conteúdo por grupo de usuários.

15.14.2.13. Configuração da unidade de alta disponibilidade.

15.14.2.14. Configuração de QoS por serviços e/ou aplicações.

15.14.2.15. Testes de funcionalidade.

15.14.3. **Configuração de switches (itens 4 e 5)**

- 15.14.3.1. Configurações básicas de conectividade.
- 15.14.3.2. Registro e ativação de licenças e Atualização de software.
- 15.14.3.3. Configuração de VLANs e roteamento interno.
- 15.14.3.4. Configurações de gerenciamento.
- 15.14.3.5. Configuração de QoS.
- 15.14.3.6. Testes de funcionalidade.
- 15.14.4. **Configuração de Access Points (item 6)**
- 15.14.4.1. Configurações básicas de conectividade.
- 15.14.4.2. Registro e ativação de licenças e Atualização de software.
- 15.14.4.3. Configuração de VLANs e roteamento interno.
- 15.14.4.4. Configuração de SSIDs.
- 15.14.4.5. Configurações de gerenciamento.
- 15.14.4.6. Configuração de QoS.
- 15.14.4.7. Testes de funcionalidade.
- 15.14.5. **Configuração de solução de XDR (item 7)**
- 15.14.5.1. Configurações básicas de conectividade.
- 15.14.5.2. Registro e ativação de licenças e Atualização de software.
- 15.14.5.3. Configuração de regras de segurança para endpoints.
- 15.14.5.4. Testes de funcionalidade.
- 15.14.6. Os serviços de instalação e configuração deverão ser executados por profissional com certificação técnica oficial emitida pelo fabricante da solução de Firewall, cuja comprovação deverá ser apresentada pela Contratada antes do início das respectivas atividades técnicas, observadas as formas de comprovação previstas no item 15.1.7 deste Termo de Referência.

15.15. ITEM 11 - TREINAMENTO OFICIAL DO FABRICANTE EM CADA UM DOS PRODUTOS FORNECIDOS TURMA DE ATÉ 2 PARTICIPANTES

- 15.15.1. Treinamento oficial no formato EAD (Ensino a Distância) para cada uma das soluções propostas:
 - 15.15.1.1. Appliance de gerenciamento centralizado (item 1) – 2 Vouchers.
 - 15.15.1.2. Firewall tipo 1 e 2 (itens 2 e 3) – 2 Vouchers.
 - 15.15.1.3. Switches Gigabit (itens 4 e 5) – 2 Vouchers.
 - 15.15.1.4. Access Points (item 6) – 2 Vouchers.
 - 15.15.1.5. Solução de detecção e resposta estendida (XDR) (item 7) – 2 Vouchers.
- 15.15.2. Deverá ser enviado link do site oficial do fabricante contendo o código ou partnumber ou SKU, além do título, carga horária e ementa de cada um dos treinamentos.
- 15.15.3. Os treinamentos de cada um dos itens serão referentes ao seu nível básico/foundation.
- 15.15.4. Os instrutores devem ser falantes do idioma português e deverão ministrar os cursos nesta língua.
 - 15.15.4.1. Pelo treinamento ser oficial, fica implícito que os instrutores deverão ser certificados para ministrar os respectivos treinamentos.
- 15.16. Deverá ser enviada uma janela de datas futuras de, no mínimo, 6 (seis) meses a partir da data de assinatura do contrato de cada um dos cursos que serão ministrados.

15.16.0.1. Será de escolha do CRM-MG as datas que lhe forem mais oportunas, podendo, eventualmente, delegar os participantes separadamente para o mesmo curso em datas diferentes.

15.16.1. Somente serão aceitos cursos ministrados por instituições de treinamento reconhecidos pelo fabricante em seu site na ocasião da assinatura do contrato.

15.16.2. Laboratórios, apostilas e demais recursos para treinamento serão responsabilidade e custeados pela instituição. Não será permitido treinamento/ hands on na solução implantada no CRM-MG.

16. ANEXO II - MODELO DE TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO

TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO

INTRODUÇÃO

O Termo de Compromisso de Manutenção de Sigilo registra o comprometimento formal da Contratada em cumprir as condições estabelecidas no documento relativas ao acesso e utilização de informações sigilosas da Contratante em decorrência de relação contratual, vigente ou não.

Referência: Art. 18, Inciso V, alínea “a” da IN SGD/ME Nº 94/2022.

Pelo presente instrumento o , sediado em , CNPJ nº , doravante denominado **CONTRATANTE**, e, de outro lado, a , sediada em , CNPJ nº , doravante denominada **CONTRATADA**;

CONSIDERANDO que, em razão do **CONTRATO** N.º , doravante denominado **CONTRATO PRINCIPAL**, a **CONTRATADA** poderá ter acesso a informações sigilosas do **CONTRATANTE**;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação e Privacidade da **CONTRATANTE**;

Resolvem celebrar o presente **TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO**, doravante **TERMO**, vinculado ao **CONTRATO PRINCIPAL**, mediante as seguintes cláusulas e condições abaixo discriminadas.

1. OBJETO

1.1. Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas disponibilizadas pela CONTRATANTE e a observância às normas de segurança da informação e privacidade por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18 de novembro de 2011, Lei nº 13.709, de 14 de agosto de 2018, e os Decretos 7.724, de 16 de maio de 2012, e 7.845, de 14 de novembro de 2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

2. CONCEITOS E DEFINIÇÕES

2.1. Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

2.2. **INFORMAÇÃO:** dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

2.3. **INFORMAÇÃO SIGILOSA:** aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquela abrangida pelas demais hipóteses legais de sigilo.

2.4. **CONTRATO PRINCIPAL:** contrato celebrado entre as partes, ao qual este TERMO se vincula.

3. DA INFORMAÇÃO SIGILOSA

3.1. Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados **INFORMAÇÕES**, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

4. DOS LIMITES DO SIGILO

4.1. As obrigações constantes deste TERMO não serão aplicadas às **INFORMAÇÕES** que:

I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

5. DIREITOS E OBRIGAÇÕES

5.1. As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas **INFORMAÇÕES**, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento prévio e expresso da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmos judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

6. VIGÊNCIA

6.1. O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

7. PENALIDADES

7.1. A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES,

devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme previsto nos arts. 155 a 163 da Lei nº. 14.133, de 2021.

8. DISPOSIÇÕES GERAIS

8.1. Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro - Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa-fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo - O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro - Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I - A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II - A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III - A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV - Todas as condições, termos e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V - O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI - Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII - O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações, conforme definição do item 3 deste documento, disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;

VIII - Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

9.1. A CONTRATANTE elege o foro da , onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

10.1. E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

CONTRATADA	CONTRATANTE

TESTEMUNHAS	

17. ANEXO III - MODELO DE TERMO DE CIÊNCIA

TERMO DE CIÊNCIA

INTRODUÇÃO

O Termo de Ciência visa obter o comprometimento formal dos empregados da Contratada diretamente envolvidos na contratação quanto ao conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes no órgão/entidade.

No caso de substituição ou inclusão de empregados da contratada, o preposto deverá entregar ao Fiscal Administrativo do Contrato os Termos de Ciência assinados pelos novos empregados envolvidos na execução dos serviços contratados.

Referência: Art. 18, Inciso V, alínea “b” da IN SGD/ME Nº 94/2022.

1 - IDENTIFICAÇÃO

CONTRATO Nº:	
OBJETO:	
CONTRATADA:	
CNPJ:	
PREPOSTO:	
GESTOR DO CONTRATO:	

2 - CIÊNCIA

2.1 Por este instrumento, os funcionários abaixo identificados declaram ter ciência e conhecer o inteiro teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes da Contratante.

Funcionários da Contratada		
Nome	Matrícula	Assinatura

Local, dia de mês de ano

18. ANEXO IV - MODELO DE TERMO DE RECEBIMENTO PROVISÓRIO

TERMO DE RECEBIMENTO PROVISÓRIO

INTRODUÇÃO

O Termo de Recebimento Provisório trata-se de termo detalhado que declarará que os serviços foram prestados e atendem às exigências de caráter técnico, sem prejuízo de posterior verificação de sua conformidade com as exigências contratuais, baseada nos requisitos e nos critérios de aceitação definidos no Modelo de Gestão do Contrato.

Referência: Inciso XXI, art. 2º, e alínea “i”, inciso II, art. 33 da IN SGD/ME Nº 94/2022.

1 - IDENTIFICAÇÃO

CONTRATO Nº:	
CONTRATADA:	
CNPJ:	
Nº DA OS:	
DATA DA EMISSÃO:	

2 - ESPECIFICAÇÃO DOS SERVIÇOS E VOLUMES DE EXECUÇÃO

SOLUÇÃO DE TIC			
Descrição da solução de TIC solicitada relacionada ao contrato anteriormente identificado			
ITEM	DESCRIÇÃO DO BEM OU SERVIÇO	MÉTRICA	QUANTIDADE
1	Descrição igual ao da OS de abertura		
TOTAL DE ITENS:			

3 - RECEBIMENTO

Para fins de cumprimento do disposto no art. 33, inciso II, alínea “i”, da IN SGD/ME nº 94/2022, por este instrumento ATESTO que os serviços correspondentes à acima identificada, conforme definido no Modelo de Execução do contrato supracitado, foram executados e atende(m)/atende(m) parcialmente/não atende(m) às respectivas exigências de caráter técnico discriminadas abaixo. Não obstante, estarão sujeitos à avaliação específica para verificação do atendimento às demais exigências contratuais, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do contrato.

Ressaltamos que o recebimento definitivo desses serviços ocorrerá somente após a verificação desses requisitos e das demais condições contratuais, desde que não se observem inconformidades ou divergências quanto às especificações constantes do Termo de Referência e do Contrato acima identificado que ensejem correções por parte da CONTRATADA. Por fim, reitera-se que o objeto poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com o contrato.

ITEM	ESPECIFICAÇÃO TÉCNICA	ATENDIMENTO	OBSERVAÇÃO
1	exigências técnicas definidas no TR		

4 - ASSINATURA

FISCAL TÉCNICO	FISCAL ADMINISTRATIVO	PREPOSTO
Nome do Fiscal Técnico do Contrato	Nome do Fiscal Administrativo do Contrato	Nome do Preposto do Contrato
		Local, dia de mês de ano.

19. ANEXO V - MODELO DE TERMO DE RECEBIMENTO DEFINITIVO

TERMO DE RECEBIMENTO DEFINITIVO

INTRODUÇÃO

O Termo de Recebimento Definitivo declarará formalmente à Contratada que os serviços prestados ou que os bens fornecidos foram devidamente avaliados e atendem às exigências contratuais, de acordo com os requisitos e critérios de aceitação estabelecidos.

Referência: Inciso XXII, Art. 2º e alínea “h” inciso I do art. 33, da IN SGD/ME Nº 94/2022.

1 - IDENTIFICAÇÃO

CONTRATO/NOTA DE EMPENHO Nº			
CONTRATADA		CNPJ	
Nº DA OS/OFB			
DATA DA EMISSÃO			

2 - ESPECIFICAÇÃO DOS PRODUTO(S)/BEM(S)/SERVIÇOS E VOLUMES DE EXECUÇÃO

SOLUÇÃO DE TIC				
Descrição da solução de TIC solicitada relacionada ao contrato anteriormente identificado				
ITEM	DESCRIÇÃO DO BEM OU SERVIÇO	MÉTRICA	QUANTIDADE	TOTAL
1	descrição igual à da OS/OFB de abertura			
TOTAL DE ITENS				

3 - ATESTE DE RECEBIMENTO

Para fins de cumprimento do disposto no art. 33, inciso II, alínea “h”, da IN SGD/ME nº 94/2022, por este instrumento ATESTO /ATESTAMOS que o(s) serviço(s)/ bem(s) correspondentes à OS/OFB acima identificada foram prestados/entregues pela e ATENDEM às exigências contratuais, discriminadas abaixo, de acordo com os Critérios CONTRATADA de Aceitação previamente definidos no Modelo de Gestão do Contrato acima indicado.

ITEM	EXIGÊNCIA CONTRATUAL	ATENDIMENTO	OBSERVAÇÃO
------	----------------------	-------------	------------

1	exigência contratual estabelecida no TR		

4 - DESCONTOS EFETUADOS E VALOR A LIQUIDAR

De acordo com os critérios de aceitação e demais termos contratuais, não há incidência de descontos por desatendimento dos indicadores de níveis de serviços definidos.

Não foram / Foram identificadas inconformidades técnicas ou de negócio que ensejam indicação de glosas e sanções, cuja instrução corre em processo administrativo próprio (nº do processo).

Por conseguinte, o valor a liquidar correspondente à OS/OFB acima identificada monta em R\$ valor (valor por extenso)

Referência: Relatório de Fiscalização nº xxxx ou Nota Técnica nº yyyy.

5 - ASSINATURA

GESTOR DO CONTRATO

Nome do Gestor do Contrato

Matrícula: xxxxxxxx

Local, dia de mês de ano.



Documento assinado eletronicamente por **Alessandro de Freitas Bartels, Gerente do Departamento de Tecnologia da Informação do CRM-MG**, em 18/08/2026, às 22:31, com fundamento no art. 5º da [RESOLUÇÃO CFM nº2.308/2022, de 28 de março de 2022](#).



A autenticidade do documento pode ser conferida no site https://sei.cfm.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **4737830** e o código CRC **83FCFD94**.



Rua dos Timbiras, 1200 - Bairro Boa Viagem |
CEP 30140-064 | Belo Horizonte/MG -
<https://www.crmmg.org.br/>



Referência: Processo SEI nº 26.13.000003312-0 | data de inclusão: 18/08/2026



CONSELHO REGIONAL DE MEDICINA DO ESTADO DE MINAS GERAIS

ESTUDO TÉCNICO PRELIMINAR - ETP

I - INFORMAÇÕES GERAIS

1. Equipe de Planejamento - Responsáveis

Nome	Cargo/função	Matrícula	E-mail
Alessandro de Freitas Bartels	Integrante Requirante	691	alessandro.bartels@crmmg.org.br
Thiago da Fonseca Duarte	Integrante Técnico	848	thiago.duarte@crmmg.org.br
Matheus Tadeu da Silveira Moreira	Integrante Administrativo	1072	matheus.moreira@crmmg.org.br

II - NECESSIDADE - DIAGNÓSTICO SITUAÇÃO ATUAL

2. Descrição do problema a ser resolvido ou da necessidade apresentada (art. 18, § 1º, I, da Lei Federal nº 14.133, de 2021).

A presente contratação tem por objetivo atender à necessidade de modernização e fortalecimento da segurança da informação no âmbito do CRM-MG, considerando a crescente dependência dos serviços institucionais em relação à infraestrutura tecnológica, à conectividade entre a Sede e as Delegacias Regionais e à proteção dos dados e sistemas corporativos.

Atualmente, a rede corporativa do CRM-MG demanda maior integração entre os mecanismos de proteção de perímetro, controle de acesso, gerenciamento de rede e proteção dos endpoints. A evolução das ameaças cibernéticas, como malwares avançados, ransomware, tentativas de acesso indevido e exploração de vulnerabilidades, exige a adoção de uma arquitetura de segurança mais moderna, integrada e centralizada, capaz de ampliar a visibilidade sobre o ambiente tecnológico e melhorar a capacidade de prevenção, detecção e resposta a incidentes.

A necessidade apresentada envolve, portanto, a implantação de uma Solução Integrada de Segurança da Informação, contemplando firewalls de próxima geração, equipamento de gerenciamento centralizado, switches, access points, solução de detecção e resposta de endpoint — XDR, licenciamento, atualizações, suporte técnico, garantia, instalação, configuração e treinamento oficial do fabricante.

A contratação busca garantir maior disponibilidade, confidencialidade e integridade das informações institucionais, proteger sistemas e serviços críticos, padronizar a infraestrutura de segurança e rede, reduzir riscos operacionais e fortalecer a governança de tecnologia da informação, em alinhamento à Lei Geral de Proteção de Dados — LGPD, às normas de compliance e às boas práticas de segurança da informação aplicáveis à Administração Pública.

Dessa forma, a solução pretendida visa substituir ou complementar recursos atualmente insuficientes ou tecnologicamente defasados, evitando a manutenção de um ambiente heterogêneo, de difícil gestão e com maior risco de falhas de interoperabilidade, indisponibilidade ou vulnerabilidades de segurança.

3. Área Requisitante

Departamento de Tecnologia da Informação

4. Descrição dos requisitos da potencial contratação (art. 18, § 1º, III, da Lei Federal nº 14.133, de 2021)

A solução pretendida deverá atender aos seguintes requisitos mínimos:

a) **Integração da solução:** ser composta por componentes compatíveis e integrados entre si, contemplando hardware, software, licenciamento, suporte, gerenciamento centralizado e funcionalidades de segurança, de modo a assegurar interoperabilidade, padronização, gestão unificada e redução de riscos decorrentes de soluções heterogêneas;

b) **Abrangência da solução:** permitir cobertura da infraestrutura tecnológica da Sede e das Delegacias Regionais do CRM-MG, considerando a necessidade de padronização, gerenciamento centralizado, proteção de perímetro, controle de acesso e segurança dos endpoints distribuídos nas unidades;

c) **Arquitetura de segurança em múltiplas camadas:** contemplar arquitetura

de segurança em múltiplas camadas, abrangendo proteção de perímetro, proteção da rede interna, controle de acesso, segurança da conectividade sem fio e proteção dos endpoints;

d) **Compatibilidade e gerenciamento centralizado:** permitir, nos componentes centrais da solução de segurança, gerenciamento centralizado, aplicação de políticas de segurança de forma padronizada, visibilidade do ambiente e administração integrada dos recursos fornecidos;

e) **Alta disponibilidade dos componentes críticos:** prever recursos de alta disponibilidade para os componentes críticos instalados na Sede, de forma a reduzir riscos de indisponibilidade dos serviços institucionais em caso de falha de equipamento ou componente essencial;

f) **Prazo de vigência, suporte e garantia:** contemplar o fornecimento de licenças, atualizações, suporte técnico e garantia pelo período mínimo de 60 (sessenta) meses. A adoção desse prazo mostra-se mais vantajosa para a Administração em razão da natureza crítica e estruturante da solução, da necessidade de continuidade da proteção da rede corporativa e dos endpoints, da redução de riscos de descontinuidade de licenças, subscrições e suporte técnico, bem como da compatibilidade com o ciclo de vida usual de equipamentos de segurança e infraestrutura de rede. Além disso, o prazo de 60 (sessenta) meses favorece a diluição dos custos de implantação, configuração, treinamento e transição, reduz a necessidade de novas contratações em curto intervalo de tempo e contribui para maior estabilidade operacional, previsibilidade orçamentária e melhor aproveitamento dos recursos públicos. Prazo inferior poderia reduzir a vantajosidade da contratação, uma vez que anteciparia a necessidade de novo procedimento de contratação ou renovação da solução, aumentaria o risco de descontinuidade operacional, reduziria o aproveitamento dos investimentos iniciais de implantação e capacitação e poderia ocasionar custos administrativos e técnicos adicionais em período incompatível com o ciclo de vida esperado da solução.

g) **Garantia da contratação:** a futura contratação deverá prever a exigência de garantia contratual, em razão da natureza crítica da Solução Integrada de Segurança da Informação, do valor estimado, da abrangência da solução na Sede e nas Delegacias Regionais e da existência de obrigações que se projetam por 60 (sessenta) meses, especialmente quanto ao licenciamento, subscrições, suporte técnico, atualizações, assistência técnica, garantia e atendimento de chamados.

h) **Firewalls de próxima geração:** contemplar firewalls de próxima geração, com funcionalidades compatíveis com a proteção de perímetro, controle de tráfego, inspeção, prevenção contra ameaças, aplicação de políticas de segurança e integração com os demais componentes da solução;

i) **Solução XDR para endpoints:** permitir proteção, monitoramento, detecção e resposta a ameaças em endpoints, incluindo recursos de análise de comportamento, correlação de eventos e identificação de atividades suspeitas, preferencialmente alinhados a modelos reconhecidos de classificação de ameaças, como MITRE ATT&CK;

j) **Equipamentos de rede:** contemplar switches e access points compatíveis com a arquitetura proposta, permitindo padronização, gerenciamento e segurança da infraestrutura de rede da Sede e das Delegacias Regionais;

k) **Atualizações, licenciamento e inteligência de ameaças:** contemplar licenciamento, atualizações, assinaturas de segurança e mecanismos de inteligência de ameaças durante todo o período de vigência, de modo a manter os recursos de proteção atualizados contra novas vulnerabilidades e ameaças

cibernéticas;

l) **Proteção contra ameaças modernas:** possuir recursos compatíveis com a prevenção, detecção e resposta a ameaças cibernéticas modernas, incluindo malwares, ransomware, acessos indevidos, exploração de vulnerabilidades e comportamentos suspeitos em endpoints e na rede;

m) **Registro, auditoria e rastreabilidade:** disponibilizar recursos de registro, consulta e auditoria de eventos, de modo a apoiar a governança de tecnologia da informação, a apuração de incidentes, a rastreabilidade de ações e o acompanhamento da postura de segurança do ambiente;

n) **Escalabilidade:** possuir capacidade de expansão, permitindo o acréscimo futuro de equipamentos, licenças ou funcionalidades, caso haja crescimento da demanda institucional, sem necessidade de substituição integral da arquitetura contratada;

o) **Garantia, manutenção e ciclo de vida:** prever garantia durante todo o período contratado e assegurar a substituição de componentes que atinjam condição de End-of-Sale, End-of-Support ou End-of-Life durante a vigência contratual, por outros com características iguais ou superiores, sem prejuízo à continuidade da solução;

p) **Suporte técnico:** contemplar suporte técnico do fabricante e/ou da contratada, conforme níveis de serviço a serem definidos no Termo de Referência, sem que o suporte prestado diretamente pelo fabricante caracterize, por si só, subcontratação indevida;

q) **Implantação e configuração:** ser planejada e executada de forma a minimizar impactos na rede em funcionamento, evitando interrupções indevidas dos serviços institucionais e garantindo cronograma de execução, testes, validações e transição adequada entre o ambiente existente e a nova solução;

r) **Equipe técnica:** prever que a licitante disponha, no momento oportuno da execução contratual, de profissionais com certificações ou qualificações compatíveis com a solução ofertada, conforme requisitos técnicos a serem detalhados no Termo de Referência;

s) **Transferência de conhecimento:** prever treinamento oficial do fabricante para a equipe técnica do CRM-MG, contemplando materiais de apoio, manuais, ambiente virtual ou físico para prática e conteúdo compatível com os produtos fornecidos, de modo a possibilitar que a equipe interna acompanhe, administre e opere os principais recursos da solução.

III - PROSPECÇÃO DE SOLUÇÕES

5. Levantamento mercadológico (que consiste na análise das alternativas possíveis, e justificativa técnica e econômica da escolha do tipo de solução a contratar) (art. 18, § 1º, V, da Lei Federal nº 14.133, de 2021).

Foram analisadas alternativas disponíveis no mercado capazes de atender à necessidade de modernização e fortalecimento da segurança da informação do CRM-MG, considerando a implantação de uma solução integrada composta por firewalls de próxima geração, gerenciamento centralizado, switches, access points, solução de detecção e resposta de endpoint — XDR, licenciamento, atualizações, suporte técnico, garantia, instalação, configuração e transferência de conhecimento.

O levantamento mercadológico considerou soluções com arquitetura integrada de segurança, capazes de atender à Sede e às Delegacias Regionais do CRM-MG, com foco na proteção de perímetro, segurança da rede interna, conectividade sem fio, proteção de endpoints, gerenciamento centralizado e melhoria da capacidade de prevenção, detecção e resposta a incidentes.

A partir das consultas realizadas junto ao mercado, identificou-se a existência de, ao menos, dois modelos possíveis para atendimento da demanda:

I - Aquisição de bens e serviços — CAPEX / investimento: modelo em que o CRM-MG adquire os equipamentos, licenças, garantias, suporte, serviços de instalação, configuração e treinamento, incorporando os bens ao seu patrimônio e mantendo a solução em operação pelo período de vigência das licenças, suporte e garantia contratados.

II - Serviço gerenciado — OPEX / pagamento recorrente: modelo em que o CRM-MG contrata o direito de uso dos equipamentos, licenças, suporte e serviços correlatos, mediante pagamento recorrente durante o período contratado, com devolução dos equipamentos ao final da vigência, conforme condições estabelecidas pelo fornecedor.

Foram obtidas propostas comerciais de fornecedores atuantes no mercado de segurança da informação e infraestrutura de rede, contemplando soluções tecnológicas integradas e comparáveis em termos de finalidade, abrangência e escopo geral. As propostas serviram como base preliminar para avaliação das alternativas possíveis, especialmente quanto à viabilidade técnica, forma de contratação, custo total estimado, continuidade da solução e impactos operacionais para o CRM-MG.

Verificou-se que o mercado dispõe de soluções integradas com gerenciamento centralizado, suporte técnico, licenciamento por prazo determinado e recursos de proteção em múltiplas camadas, inclusive com funcionalidades de firewall de próxima geração e XDR. Também se observou que a integração entre os componentes é fator relevante para reduzir riscos de incompatibilidade, simplificar a administração, favorecer a padronização das políticas de segurança e ampliar a visibilidade sobre o ambiente tecnológico.

Dessa forma, o levantamento mercadológico demonstrou a existência de alternativas viáveis para atendimento da necessidade, permitindo a comparação entre o modelo de aquisição dos bens e serviços e o modelo de serviço gerenciado. A análise comparativa das alternativas identificadas é apresentada no item seguinte deste Estudo Técnico Preliminar.

6. Comparativo das soluções

A escolha entre a aquisição de bens e serviços — modelo CAPEX — e a contratação de serviço gerenciado — modelo OPEX — representa decisão relevante para o CRM-MG, pois impacta diretamente a gestão financeira, operacional e patrimonial

da solução pretendida.

No modelo de aquisição de bens e serviços — CAPEX, o CRM-MG realiza investimento inicial para aquisição dos equipamentos, licenças, garantias, suporte técnico, serviços de instalação, configuração e treinamento. Essa alternativa permite que os bens sejam incorporados ao patrimônio institucional, assegura maior controle sobre os ativos e possibilita sua utilização durante todo o período de vigência das licenças, suporte e garantia contratados. Além disso, reduz o risco de descontinuidade decorrente da necessidade de devolução dos equipamentos ao final da vigência contratual.

Como desvantagem, o modelo CAPEX exige maior desembolso inicial e impõe à Administração a necessidade de realizar adequado planejamento orçamentário para suportar o investimento. Também demanda controle patrimonial, gestão do ciclo de vida dos equipamentos e planejamento futuro para eventual substituição, atualização ou desfazimento dos ativos ao final de sua vida útil.

No modelo de serviço gerenciado — OPEX, o CRM-MG contrata o direito de uso dos equipamentos, licenças, suporte e serviços correlatos, mediante pagamento recorrente durante o prazo contratual. Essa alternativa pode trazer maior previsibilidade de desembolso mensal, reduzir a necessidade de investimento inicial elevado e transferir parte da responsabilidade de gestão dos ativos ao fornecedor.

Entretanto, no modelo OPEX, os equipamentos não passam a integrar o patrimônio do CRM-MG e, em regra, devem ser devolvidos ao final da vigência contratual. Essa característica pode gerar risco operacional relevante, especialmente porque os componentes da solução constituem base essencial para o funcionamento da rede corporativa e para a segurança da informação. Assim, eventual atraso em nova contratação, substituição de fornecedor ou descontinuidade contratual poderia exigir planejamento adicional, transição complexa e risco de interrupção ou degradação dos serviços institucionais.

A partir do levantamento mercadológico com fornecedores distintos, que apresentaram alternativas tanto para aquisição quanto para serviço gerenciado, foram obtidos os seguintes valores estimados para cada cenário:

Cenário 1 — Aquisição de bens e serviços — CAPEX

Fornecedor	Valor
Altasnet	R\$ 2.727.052,00
Secureway	R\$ 1.248.802,93
Teltec	R\$ 4.654.700,00
Valor médio	R\$ 2.876.851,64

Cenário 2 — Serviço gerenciado — OPEX

Fornecedor	Valor estimado após 60 meses
Altasnet	R\$ 3.226.080,00
Secureway	R\$ 3.120.000,00
Teltec	R\$ 5.341.010,78
Valor médio	R\$ 3.895.696,93

Observa-se que, sob o aspecto econômico, o modelo de aquisição de bens e serviços — CAPEX apresenta menor custo total estimado para o período de 60 meses. Considerando os valores médios apurados, o modelo de serviço gerenciado — OPEX representa custo aproximadamente 36% superior ao modelo de aquisição.

Quanto à eficiência administrativa, embora o modelo OPEX possa reduzir o desembolso inicial e simplificar parte da gestão patrimonial, o modelo CAPEX se mostra mais adequado à realidade do CRM-MG por assegurar maior controle sobre os ativos essenciais à operação da rede, permitir planejamento mais estável da infraestrutura e reduzir riscos associados à devolução dos equipamentos ao final do contrato.

Em relação à continuidade sustentável da prestação dos serviços, o modelo CAPEX também se mostra mais favorável, uma vez que os equipamentos permanecerão sob domínio do CRM-MG durante o ciclo de vida contratado, reduzindo a dependência de transição imediata ao término da vigência. Essa condição é especialmente relevante porque a solução pretendida envolve componentes críticos de segurança, conectividade e proteção da rede corporativa.

Sob o aspecto tecnológico, ambos os modelos são capazes de atender à necessidade institucional, desde que contemplem firewalls de próxima geração, gerenciamento centralizado, switches, access points, solução XDR, licenciamento, atualizações, suporte, garantia, instalação, configuração e transferência de conhecimento. Dessa forma, a diferenciação entre os modelos não está na capacidade técnica essencial da solução, mas principalmente no custo total estimado, na forma de disponibilização dos ativos, no grau de controle pela Administração e nos riscos de continuidade ao final da vigência.

Quanto à sustentabilidade, em ambos os cenários deverão ser observadas medidas relacionadas ao consumo eficiente de energia, ao ciclo de vida dos equipamentos e ao descarte ambientalmente adequado dos bens substituídos. No modelo CAPEX, tais medidas deverão ser consideradas na gestão patrimonial e no futuro desfazimento dos equipamentos. No modelo OPEX, deverão ser observadas as responsabilidades do fornecedor quanto à destinação adequada dos bens ao final do contrato.

Não foram identificadas, para o caso concreto, alternativas menos onerosas, como doação, permuta ou chamamento público, capazes de atender de forma adequada à necessidade institucional, considerando a criticidade da solução, a necessidade de garantia, suporte técnico, atualizações, licenciamento, integração e continuidade operacional.

Diante da comparação realizada, verifica-se que o modelo de aquisição de bens e serviços — CAPEX apresenta, para o caso concreto, melhor aderência às necessidades do CRM-MG, especialmente por apresentar menor custo total estimado no horizonte de 60 meses, permitir maior controle sobre os ativos essenciais à segurança e à operação da rede corporativa, reduzir riscos relacionados à devolução de equipamentos ao final da vigência contratual e favorecer a continuidade operacional da solução. Assim, a alternativa de aquisição mostra-se, no comparativo realizado, mais vantajosa que o modelo de serviço gerenciado, ficando a descrição da solução escolhida detalhada no item seguinte deste Estudo Técnico Preliminar.

7. Descrição da solução escolhida (art. 18, § 1º, VII, da Lei Federal nº 14.133, de 2021)

Diante da análise realizada nos itens anteriores, a solução escolhida consiste na contratação de Solução Integrada de Segurança da Informação, no modelo de aquisição de bens e serviços — CAPEX, contemplando o fornecimento, implantação, configuração, suporte técnico, garantia, licenciamento, atualizações e transferência de conhecimento, pelo período mínimo de 60 (sessenta) meses.

A solução deverá abranger firewalls de próxima geração, equipamento de gerenciamento centralizado, switches, access points, solução de detecção e resposta de endpoint — XDR, licenciamento, atualizações, suporte técnico do fabricante e/ou da contratada, garantia, serviço de instalação e configuração, bem como treinamento oficial do fabricante para a equipe técnica do CRM-MG.

A escolha pelo modelo de aquisição justifica-se por apresentar, no comparativo realizado, menor custo total estimado no horizonte de 60 meses, maior controle institucional sobre os ativos, melhor aderência à necessidade de continuidade operacional da rede corporativa e menor exposição a riscos decorrentes da devolução de equipamentos ao final da vigência contratual, situação observada no modelo de serviço gerenciado.

A solução escolhida deverá atender à Sede e às Delegacias Regionais do CRM-MG, possibilitando a padronização da infraestrutura de segurança e rede, o gerenciamento centralizado dos componentes, a aplicação uniforme de políticas de segurança, a proteção dos endpoints e a ampliação da capacidade de prevenção, detecção e resposta a incidentes de segurança da informação.

Considerando a natureza integrada da solução, a contratação deverá ser estruturada de forma a contemplar todos os componentes necessários ao seu funcionamento harmônico, incluindo equipamentos, licenças, serviços de implantação, configuração, suporte, garantia, atualizações e treinamento. Dessa forma, não se identifica, neste momento, a necessidade de contratações autônomas adicionais para viabilizar a implantação inicial da solução, sem prejuízo de eventuais providências administrativas internas necessárias à execução contratual.

A descrição técnica detalhada dos componentes, dos níveis de serviço, das condições de execução, dos critérios de aceitação, das responsabilidades da contratada e das demais obrigações necessárias será desenvolvida posteriormente no Termo de Referência, a ser elaborado na etapa subsequente do planejamento da contratação.

8. Estimativas das quantidades para contratação, acompanhadas de memórias de cálculo e dos documentos que lhe dão suporte (considerar interdependências com outras contratações, de modo a possibilitar economia de escala) (art. 18, § 1º, IV, da Lei Federal nº 14.133, de 2021).

As quantidades estimadas para a contratação foram definidas com base na necessidade de cobertura da infraestrutura tecnológica da Sede e das 20 Delegacias Regionais do CRM-MG, bem como no quantitativo atual de endpoints, compreendendo estações de trabalho e servidores que deverão ser protegidos pela solução de detecção e resposta de endpoint — XDR.

A estimativa considera a necessidade de implantação de componentes centrais de segurança e gerenciamento na Sede, a disponibilização de equipamentos de proteção, conectividade cabeada e conectividade sem fio para as Delegacias Regionais, a padronização da infraestrutura de rede e segurança, o licenciamento, as atualizações, o suporte técnico, a garantia pelo período de 60 (sessenta) meses, os serviços de instalação e configuração e a transferência de conhecimento à equipe técnica do CRM-MG.

Para os firewalls, considerou-se a necessidade de equipamentos de maior capacidade para a Sede, em quantidade suficiente para permitir estrutura de alta disponibilidade dos componentes críticos, e de equipamentos adequados ao porte das 20 Delegacias Regionais. Para os switches de 16 portas e access points internos tipo 2, considerou-se a necessidade de atendimento das 20 Delegacias Regionais, com previsão de 1 equipamento de cada tipo por unidade. Para os switches de 8 portas com PoE e access points internos tipo 1, as quantidades foram estimadas de acordo com a necessidade de atualização, padronização e ampliação da infraestrutura de rede cabeada e sem fio, especialmente na Sede e em pontos que demandem características específicas de conectividade. Para a solução XDR, foi considerado o quantitativo estimado de 330 endpoints a serem protegidos.

As quantidades estimadas são apresentadas no quadro a seguir:

Item	Descrição do item	Quantidade	Métrica / memória de cálculo
1	Equipamento de gerenciamento centralizado — appliance	1	Unidade central de gerenciamento da solução
2	Firewall tipo 1	2	Equipamentos destinados à Sede, considerando necessidade de alta disponibilidade dos componentes críticos
3	Firewall tipo 2	20	Equipamentos destinados às 20 Delegacias Regionais
4	Switch gigabit de 8 portas com PoE	7	Equipamentos destinados à atualização e padronização da infraestrutura de rede em pontos que demandem alimentação PoE
5	Switch gigabit de 16 portas	20	Equipamentos destinados às 20 Delegacias Regionais, considerando 1 unidade por Delegacia
6	Access point interno tipo 1	30	Equipamentos destinados à cobertura e padronização da conectividade sem fio, conforme necessidade da infraestrutura abrangida pela solução
7	Access point interno tipo 2	20	Equipamentos destinados às 20 Delegacias Regionais, considerando 1 unidade por Delegacia

Item	Descrição do item	Quantidade	Métrica / memória de cálculo
8	Solução de detecção e resposta de endpoint — XDR	330	Licenças/unidades, considerando o quantitativo estimado de endpoints a serem protegidos
9	Licenciamento, atualizações, suporte 24x7 do fabricante e garantia de 60 meses para toda a solução	1	Conjunto de serviços necessário ao funcionamento, atualização, suporte e garantia da solução pelo período contratado
10	Instalação e configuração da solução	1	Serviço necessário à implantação, configuração, testes e ativação da solução
11	Treinamento oficial do fabricante em cada produto fornecido para uma turma de até 2 participantes	1	Turma destinada à transferência de conhecimento à equipe técnica do CRM-MG

9. Estimativa do valor da contratação (art. 18, § 1º, VI, da Lei Federal nº 14.133, de 2021).

A estimativa preliminar do valor da contratação foi elaborada com base nas propostas comerciais obtidas junto a fornecedores atuantes no mercado de segurança da informação e infraestrutura de rede, considerando o modelo de aquisição de bens e serviços — CAPEX, escolhido nos itens anteriores deste Estudo Técnico Preliminar.

Os valores apresentados contemplam, de forma integrada, os equipamentos, licenças, atualizações, suporte técnico, garantia pelo período de 60 (sessenta) meses, serviço de instalação e configuração e treinamento oficial do fabricante, conforme escopo estimado para atendimento da Sede e das Delegacias Regionais do CRM-MG.

Ressalta-se que a presente estimativa tem caráter preliminar e visa subsidiar a análise de viabilidade econômico-financeira da contratação, não se confundindo, necessariamente, com a pesquisa formal de preços que poderá ser consolidada em etapa própria da instrução processual, observadas as normas aplicáveis.

A partir das propostas obtidas, foram identificados os seguintes valores referenciais:

Item	Descrição do Item	Qtde	Métrica/ Notas	Altasnet (R\$)	Secureway (R\$)	Teltec (R\$)
1	Equipamento de gerenciamento centralizado (Appliance)	1	Unidade	434.726,00	Incluso no firewall Tipo 1	143.000,00
2	Firewall Tipo 1	2	Unidades	103.936,00	89.027,37	794.000,00
3	Firewall Tipo 2	20	Unidades	63.360,00	223.126,32	636.000,00
4	Switch Gigabit de 8 Portas com PoE	7	Unidades	28.686,00	87.823,76	84.700,00

Item	Descrição do Item	Qtde	Métrica/ Notas	Altasnet (R\$)	Secureway (R\$)	Teltec (R\$)
5	Switch Gigabit de 16 Portas	20	Unidades	143.540,00	505.140,84	860.000,00
6	Access Point Interno Tipo 1	30	Unidades	111.180,00	133.703,46	540.000,00
7	Access Point Interno Tipo 2	20	Unidades	74.120,00	46.410,84	
8	Solução de Detecção e Resposta de Endpoint (XDR)	330	Licenças/ Unidades	797.610,00	34.570,80	1.280.000,00
9	Licenciamento, Atualizações, Suporte (24x7) do Fabricante e Garantia de 60 Meses para Toda a Solução	1	Conjunto (Serviço)	796.806,00	Incluso nos itens propostos	Incluso nos itens propostos
10	Instalação e Configuração da Solução	1	Serviço	94.366,00	129.000,00	300.000,00
11	Treinamento Oficial do Fabricante em Cada Produto Fornecido para uma Turma de até 2 Participantes	1	Turma (até 2 participantes)	78.722,00	Sem custo	17.000,00
Total				2.727.052,00	1.248.802,93	4.654.700,00

Considerando os valores apresentados, a estimativa preliminar da contratação, no modelo de aquisição de bens e serviços — CAPEX, corresponde ao valor médio de **R\$ 2.876.851,64**. Esse valor será utilizado como referência para a análise de viabilidade da solução neste Estudo Técnico Preliminar, sem prejuízo de posterior refinamento da pesquisa de preços na etapa própria da instrução da contratação.

10. Justificativas para o parcelamento ou não da contratação (art. 18, § 1º, VIII, da Lei Federal nº 14.133, de 2021)

A contratação não deverá ser parcelada, devendo o objeto ser estruturado como Solução Integrada de Segurança da Informação, em lote único, contemplando os equipamentos, licenças, atualizações, suporte técnico, garantia, instalação, configuração e transferência de conhecimento necessários ao funcionamento da solução.

Embora o parcelamento seja, em regra, medida voltada à ampliação da competitividade, no caso concreto a divisão do objeto em itens ou lotes independentes poderia comprometer a integração técnica da solução, a interoperabilidade entre os componentes, a padronização das políticas de segurança, o gerenciamento centralizado e a adequada responsabilização pela implantação e pelo funcionamento do conjunto.

A solução pretendida envolve componentes interdependentes, tais como firewalls de próxima geração, equipamento de gerenciamento centralizado, switches, access points, solução de detecção e resposta de endpoint — XDR, licenciamento, atualizações, suporte, garantia e serviços de instalação e configuração. Esses elementos devem operar de forma coordenada, com gestão unificada e compatibilidade entre si, a fim de assegurar a proteção da rede corporativa, a segurança dos endpoints, a visibilidade do ambiente e a continuidade dos serviços institucionais.

O parcelamento poderia gerar risco de contratação de componentes heterogêneos, com diferentes fornecedores responsáveis por partes distintas da solução, dificultando a identificação de responsabilidades em caso de falhas, incidentes, incompatibilidades, indisponibilidades ou problemas de desempenho. Também poderia aumentar a complexidade da implantação, da integração, do suporte técnico e da manutenção da solução ao longo da vigência contratual.

Além disso, a contratação em lote único favorece a economia de escala, a padronização tecnológica, a redução de riscos operacionais, a simplificação da gestão contratual e a obtenção de suporte coordenado para todos os componentes fornecidos. Essa estrutura também contribui para preservar a continuidade operacional da rede corporativa e a efetividade da arquitetura de segurança em múltiplas camadas pretendida pelo CRM-MG.

Dessa forma, diante da natureza integrada e interdependente da solução, entende-se tecnicamente justificada a não adoção do parcelamento, sendo mais adequado que a contratação seja realizada em lote único, sem prejuízo da necessária observância à competitividade e à compatibilidade dos requisitos técnicos com as práticas de mercado.

11. Contratações correlatas e/ou interdependentes (art. 18, § 1º, XI, da Lei Federal nº 14.133, de 2021)

Não foram identificadas, neste momento, contratações interdependentes indispensáveis à implantação inicial da Solução Integrada de Segurança da Informação, uma vez que o objeto pretendido já contempla, de forma integrada, o fornecimento dos equipamentos, licenças, atualizações, suporte técnico, garantia, instalação, configuração e transferência de conhecimento necessários ao funcionamento da solução.

Embora a solução se relacione com a infraestrutura tecnológica existente do CRM-MG, incluindo conectividade, ambiente de rede, serviços corporativos, servidores, estações de trabalho e demais recursos de tecnologia da informação, tais elementos já compõem o ambiente institucional em operação e não configuram, neste estudo, contratações autônomas necessárias à viabilização da presente demanda.

Eventuais ajustes internos de infraestrutura, parametrizações, janelas de implantação, validações técnicas, regras de acesso, adequações de rede ou atividades de transição deverão ser tratados como providências administrativas e técnicas de preparação e execução da contratação, sem caracterizar, neste momento, necessidade de contratação correlata ou interdependente adicional.

Dessa forma, conclui-se que não há contratações correlatas ou interdependentes a serem previamente realizadas para viabilizar a contratação pretendida, sem prejuízo de reavaliação na etapa de elaboração do Termo de Referência, caso sejam identificadas necessidades complementares decorrentes do detalhamento técnico da solução.

12. Demonstração da previsão da contratação com o Plano Anual de Compras (art. 18, § 1º, II, da Lei Federal nº 14.133, de 2021).

A contratação da Solução Integrada de Segurança da Informação está prevista no Plano Anual de Compras do CRM-MG, conforme indicado no Documento de Oficialização da Demanda, que registra a previsão de aquisição para julho de 2026.

A demanda encontra-se alinhada ao planejamento institucional do CRM-MG, especialmente quanto à necessidade de modernização da infraestrutura tecnológica, fortalecimento da segurança da informação, proteção dos dados institucionais, ampliação da capacidade de prevenção, detecção e resposta a incidentes e padronização dos recursos de segurança e rede da Sede e das Delegacias Regionais.

Registra-se que o valor inicialmente utilizado para fins de planejamento orçamentário e de inclusão ou alteração no Plano de Contratações Anual poderá ser ajustado em razão da atualização da pesquisa de preços na etapa subsequente da instrução processual, especialmente considerando a necessidade de renovação dos orçamentos utilizados na fase preliminar deste Estudo Técnico Preliminar.

Caso a atualização da estimativa de preços resulte em alteração relevante do valor da contratação, deverão ser adotadas as providências administrativas cabíveis para adequação do Projeto Orçamentário e, se necessário, dos registros do Plano de Contratações Anual, de modo a preservar a coerência entre o planejamento da contratação, a disponibilidade orçamentária e o valor estimado a ser utilizado no Termo de Referência.

IV - SOLUÇÃO ESCOLHIDA

13. Resultados pretendidos (art. 18, § 1º, IX, da Lei Federal nº 14.133, de 2021)

Com a contratação da Solução Integrada de Segurança da Informação, pretende-se elevar o nível de proteção da infraestrutura tecnológica do CRM-MG, ampliando a capacidade institucional de prevenção, detecção e resposta a ameaças cibernéticas, bem como fortalecendo a disponibilidade, a confidencialidade e a integridade dos dados e sistemas corporativos.

A solução deverá proporcionar maior controle e visibilidade sobre o ambiente tecnológico da Sede e das Delegacias Regionais, permitindo o gerenciamento centralizado dos componentes de segurança e rede, a aplicação padronizada de políticas de segurança, o acompanhamento de eventos e alertas e o apoio à rastreabilidade e à apuração de incidentes.

Também se espera obter maior eficiência operacional, mediante a padronização da infraestrutura, a redução de riscos decorrentes de soluções heterogêneas, a simplificação da administração dos recursos tecnológicos e a melhoria da capacidade de atuação da equipe técnica do CRM-MG na gestão da segurança da informação.

A contratação busca, ainda, modernizar parte dos ativos de rede atualmente utilizados, incluindo equipamentos de proteção de perímetro, conectividade cabeada, conectividade sem fio e proteção de endpoints, contribuindo para a melhoria da qualidade dos serviços tecnológicos prestados às áreas internas e para a continuidade dos serviços institucionais.

Sob o aspecto econômico, pretende-se obter melhor aproveitamento dos recursos financeiros disponíveis por meio da aquisição de solução integrada com menor custo total estimado no horizonte analisado, conforme comparativo realizado neste Estudo Técnico Preliminar, além de reduzir riscos de descontinuidade ou necessidade de substituições emergenciais decorrentes de obsolescência tecnológica.

Outro resultado pretendido é a ampliação da autonomia técnica da equipe do CRM-MG, por meio da transferência de conhecimento e do treinamento oficial do fabricante, possibilitando melhor acompanhamento, administração e operação dos principais recursos da solução durante sua vigência.

Dessa forma, os principais resultados esperados são: fortalecimento da segurança da informação; modernização e padronização da infraestrutura de segurança e rede; maior visibilidade e controle do ambiente tecnológico; melhoria da capacidade de resposta a incidentes; redução de riscos operacionais; melhor aproveitamento dos recursos humanos, materiais e financeiros; e incremento da continuidade e da qualidade dos serviços institucionais suportados pela tecnologia da informação.

14. Providências a serem adotadas pela Administração previamente à celebração do contrato (art. 18, § 1º, X, da Lei Federal nº 14.133, de 2021)

Previamente à celebração do contrato, deverão ser adotadas providências administrativas e técnicas necessárias à adequada instrução, implantação e acompanhamento da Solução Integrada de Segurança da Informação.

Inicialmente, deverá ser promovida a atualização da pesquisa de preços, considerando a necessidade de utilização de orçamentos válidos e compatíveis com a etapa de elaboração do Termo de Referência e com a futura licitação. Caso a atualização dos valores resulte em alteração relevante da estimativa da contratação, deverão ser adotadas as providências cabíveis para adequação do Projeto Orçamentário e, se necessário, dos registros do Plano de Contratações Anual — PCA.

Também deverá ser assegurada a disponibilidade orçamentária compatível com o valor estimado da contratação, observando-se o resultado da pesquisa de preços atualizada e os procedimentos internos aplicáveis ao planejamento orçamentário do CRM-MG.

No aspecto técnico, a Administração deverá realizar o levantamento e a validação das informações necessárias à implantação da solução, incluindo topologia básica da rede, unidades contempladas, quantitativo de endpoints, equipamentos atualmente em uso, regras de acesso relevantes, necessidades de conectividade, janelas de manutenção e eventuais restrições operacionais da Sede e das Delegacias Regionais.

A Administração deverá, ainda, planejar a transição entre o ambiente atual e a nova solução, em conjunto com a futura contratada, de modo a minimizar riscos de interrupção dos serviços institucionais. Para isso, deverão ser definidas janelas de implantação, cronograma de execução, procedimentos de testes, critérios de validação e estratégia de retorno, quando aplicável.

Considerando a criticidade da infraestrutura de rede e segurança, as atividades de instalação, configuração, substituição ou migração de componentes deverão ser programadas, preferencialmente, em horários de menor impacto para o funcionamento do CRM-MG, podendo envolver execução em período noturno, finais de semana ou feriados, conforme necessidade técnica e conveniência administrativa.

Por fim, deverá ser planejada a participação da equipe técnica do CRM-MG nas atividades de implantação, validação e transferência de conhecimento, de modo a permitir o acompanhamento adequado da execução contratual e a posterior administração dos principais recursos da solução.

15. Possíveis impactos ambientais e respectivas medidas mitigadoras (art. 18, § 1º, XII, da Lei Federal nº 14.133, de 2021)

A contratação poderá gerar impactos ambientais relacionados principalmente ao fornecimento, substituição, operação e posterior desfazimento de equipamentos eletroeletrônicos, tais como firewalls, switches, access points, appliance de gerenciamento e demais componentes necessários à implantação da Solução Integrada de Segurança da Informação.

Entre os possíveis impactos ambientais, destacam-se o consumo de energia elétrica durante a operação dos equipamentos, a geração de resíduos eletroeletrônicos decorrentes da substituição de ativos obsoletos ou ao final de sua vida útil, a utilização de embalagens e materiais de acondicionamento durante o fornecimento dos bens e a necessidade de destinação ambientalmente adequada dos equipamentos eventualmente substituídos.

Como medidas mitigadoras, deverão ser priorizadas soluções que observem critérios de eficiência energética, menor consumo de energia, durabilidade, garantia estendida, atualização tecnológica e suporte durante todo o ciclo contratado, contribuindo para a redução da necessidade de substituições prematuras e para o melhor aproveitamento dos recursos públicos.

Também deverão ser previstas medidas relacionadas à destinação ambientalmente adequada dos equipamentos e materiais substituídos, observadas as normas aplicáveis ao desfazimento de bens eletroeletrônicos, à logística reversa e à reciclagem, quando cabível. A futura contratação poderá prever, conforme detalhamento a ser realizado no Termo de Referência, obrigações da contratada quanto à orientação, recolhimento, destinação ou apoio à logística reversa dos componentes fornecidos ou substituídos, especialmente nos casos em que houver substituição de equipamentos durante a vigência contratual.

Quanto às embalagens e materiais utilizados no fornecimento dos equipamentos, recomenda-se que sejam adotadas práticas que favoreçam a redução de resíduos, o reaproveitamento, a reciclagem e a destinação ambientalmente adequada, sempre que tecnicamente possível e compatível com o objeto.

Dessa forma, os impactos ambientais identificados são considerados passíveis de mitigação mediante a adoção de critérios de eficiência energética, gestão adequada do ciclo de vida dos equipamentos, logística reversa, reciclagem e destinação ambientalmente correta dos resíduos eletroeletrônicos, sem prejuízo de detalhamento das exigências de sustentabilidade na etapa de elaboração do Termo de Referência.

V - VIABILIDADE

16. Posicionamento conclusivo sobre a adequação da contratação para o atendimento da necessidade a que se destina (art. 18, § 1º, XIII, da Lei Federal nº 14.133, de 2021)

Com base na análise realizada neste Estudo Técnico Preliminar, conclui-se que a contratação da Solução Integrada de Segurança da Informação, no modelo de aquisição de bens e serviços — CAPEX, mostra-se adequada, viável e razoável para o atendimento da necessidade identificada pelo CRM-MG.

A solução pretendida é tecnicamente adequada por contemplar arquitetura integrada de segurança, abrangendo firewalls de próxima geração, equipamento de gerenciamento centralizado, switches, access points, solução de detecção e resposta de endpoint — XDR, licenciamento, atualizações, suporte técnico, garantia, instalação, configuração e transferência de conhecimento. Esses componentes são compatíveis com a necessidade de modernização da infraestrutura tecnológica, proteção da Sede e das Delegacias Regionais, padronização da rede, fortalecimento da segurança da informação e ampliação da capacidade de prevenção, detecção e resposta a incidentes.

Sob o aspecto econômico, a alternativa de aquisição demonstrou, no comparativo realizado, melhor relação de vantajosidade em relação ao modelo de serviço gerenciado, especialmente por apresentar menor custo total estimado no horizonte analisado, permitir maior controle institucional sobre os ativos e reduzir riscos associados à devolução de equipamentos ao final da vigência contratual.

Registra-se que a estimativa de valor utilizada neste ETP possui caráter preliminar, tendo sido elaborada com base nos orçamentos disponíveis na fase inicial do estudo. A pesquisa de preços deverá ser atualizada e consolidada na etapa de elaboração do Termo de Referência, podendo ensejar ajustes no Projeto Orçamentário e, se necessário, nos registros do Plano de Contratações Anual — PCA, de modo a preservar a coerência entre o planejamento da contratação, a disponibilidade orçamentária e o valor estimado final.

Dessa forma, entende-se que a contratação é técnica e economicamente viável, sendo recomendada a continuidade da instrução processual, com a elaboração do Termo de Referência e demais documentos necessários à realização do procedimento de contratação.

Belo Horizonte, 01 de junho de 2026



Documento assinado eletronicamente por **Alessandro de Freitas Bartels, Gerente do Departamento de Tecnologia da Informação do CRM-MG**, em 27/07/2026, às 16:38, com fundamento no art. 5º da [RESOLUÇÃO CFM nº2.308/2022, de 28 de março de 2022](#).



Documento assinado eletronicamente por **Thiago da Fonseca Duarte, Administrador de Redes**, em 28/07/2026, às 10:04, com fundamento no art. 5º da [RESOLUÇÃO CFM nº2.308/2022, de 28 de março de 2022](#).



Documento assinado eletronicamente por **Matheus Tadeu da Silveira Moreira, Analista de Licitação**, em 28/07/2026, às 10:13, com fundamento no art. 5º da [RESOLUÇÃO CFM nº2.308/2022, de 28 de março de 2022](#).



Documento assinado eletronicamente por **Robertson Correia Bernardo, Diretor do Setor de Tecnologia da Informação e Comunicação do CRM-MG**, em 28/07/2026, às 14:43, com fundamento no art. 5º da [RESOLUÇÃO CFM nº2.308/2022, de 28 de março de 2022](#).



A autenticidade do documento pode ser conferida no site https://sei.cfm.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **4217965** e o código CRC **F5DC89DC**.



Rua dos Timbiras, 1200 - Bairro Boa Viagem |
CEP 30140-064 | Belo Horizonte/MG -
<https://www.crmmg.org.br/>



Referência: Processo SEI nº 26.13.000003312-0 | data de inclusão: 12/05/2026



CONSELHO REGIONAL DE MEDICINA DO ESTADO DE MINAS GERAIS

MINUTA DE CONTRATO

Belo Horizonte, 13 de agosto de 2026

ANEXO II - TERMO DE CONTRATO

(Processo Administrativo SEI Nº.26.13.000003312-0)

CONTRATO ADMINISTRATIVO QUE FAZEM ENTRE SI O CONSELHO REGIONAL DE MEDICINA E A EMPRESA

O **Conselho Regional de Medicina do Estado de Minas Gerais**, com sede na Rua dos Timbiras, Nº 1200, Bairro Boa Viagem, na cidade de Belo Horizonte - MG, CEP 30.140.064, inscrito no CNPJ sob o nº 22.256.879/0001-70, neste ato representado por seu Presidente, **Cons. Ricardo Hernane Lacerda Gonçalves de Oliveira**, doravante denominado CONTRATANTE, e de outro lado, a empresa _____, inscrita no CNPJ sob o nº _____, sediada à _____, doravante designado CONTRATADO, neste ato representada por _____, conforme atos constitutivos OU procuração apresentada nos autos, tendo em vista o que consta no **Processo SEI Nº. 26.13.000003312-0** 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 do **Pregão nº 13/2026**, mediante as cláusulas e condições a seguir enunciadas.

CLÁUSULA PRIMEIRA - DO OBJETO

1.1. O objeto do presente instrumento é a Aquisição de Solução Integrada de Segurança da Informação, em lote único, contemplando o fornecimento, implantação, configuração, suporte técnico, garantia, licenciamento, atualizações e transferência de conhecimento, pelo período de 60 (sessenta) meses, incluindo firewalls de próxima geração, equipamento de gerenciamento centralizado, switches, access points, solução de detecção e resposta de endpoint — XDR, serviço de instalação e configuração e treinamento oficial do fabricante nas condições estabelecidas no Termo de Referência.

1.2. Objeto da contratação:

ITEM	ESPECIFICAÇÃO	CATMAT/CATSER	UNIDADE DE MEDIDA	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	Equipamento de gerenciamento centralizado — appliance	618980	unidade	1	R\$	R\$
2	Firewall - tipo 1	609340	unidade	2	R\$	R\$
3	Firewall - tipo 2	609340	unidade	20	R\$	R\$

4	Switch gigabit de 8 portas com PoE	626423	unidade	7	R\$	R\$
5	Switch gigabit de 16 portas	300719	unidade	20	R\$	R\$
6	Access point interno - tipo 1	603936	unidade	30	R\$	R\$
7	Access point interno - tipo 2	603936	unidade	20	R\$	R\$
8	Solução de detecção e resposta de endpoint — XDR	27472	licença/unidade	330	R\$	R\$
9	Licenciamento, atualizações, suporte 24x7 do fabricante e garantia de 60 meses para toda a solução	27740	serviço	1	R\$	R\$
10	Instalação e configuração da solução	26972	serviço	1	R\$	R\$
11	Treinamento oficial do fabricante em cada produto fornecido, para turma de até 2 participantes	3840	serviço	1	R\$	R\$
Total:						R\$

1.3. Vinculam esta contratação, independentemente de transcrição:

1.3.1. O Termo de Referência;

1.3.2. O Edital da Licitação;

1.3.3. A Proposta do contratado;

1.3.4. Eventuais anexos dos documentos supracitados.

CLÁUSULA SEGUNDA - DA VIGÊNCIA

2.1. O presente contrato entra em vigor na **data de sua assinatura**, devendo ter sua eficácia e produção de efeitos condicionadas à publicação no Portal Nacional de Contratações Públicas (PNCP), nos termos do art. 94 da Lei nº 14.133, de 2021, cobrindo expressamente as etapas de fornecimento, instalação, configuração, testes, validação e aceite da solução.

2.2. O prazo integral de 60 (sessenta) meses relativo à garantia técnica, suporte, licenciamento, atualizações e manutenção terá sua contagem iniciada formalmente a partir da emissão do Termo de Recebimento Definitivo do objeto, assegurando a preservação integral do período de garantia e suporte prestado.

2.3. A vigência contratual total poderá ser prorrogada por até 10 (dez) anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021.

2.4. A prorrogação de que trata o item 2.3 é condicionada à avaliação, por parte do Gestor do Contrato, da vantajosidade da prorrogação, a qual deverá ser realizada motivadamente, com base no Histórico de Gestão do Contrato, nos princípios da manutenção da necessidade, economicidade e oportunidade da contratação, e nos demais aspectos que forem julgados relevantes, atentando, ainda, para o cumprimento dos seguintes requisitos:

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

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

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

2.4.4. Haja manifestação expressa do CONTRATADO informando o interesse na prorrogação;

2.4.5. Seja comprovado que o CONTRATADO mantém as condições iniciais de habilitação; e

2.4.6. Não haja registro no Cadastro Informativo de créditos não quitados do setor público federal (Cadin).

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

2.6. A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo, cuja eficácia também fica sujeita à divulgação no PNCP.

2.7. Nas eventuais prorrogações contratuais, a renovação abrangerá exclusivamente as obrigações de natureza continuada previstas no **item 9**, observadas as seguintes condições:

2.7.1. Os custos não renováveis (investimentos iniciais, bens de capital ou serviços pontuais) já pagos ou amortizados ao longo do primeiro período de vigência deverão ser reduzidos ou eliminados da planilha de custos como condição indispensável para a prorrogação.

2.7.2. A renovação do contrato **não** abrangerá:

a) Nova aquisição dos equipamentos e insumos referentes aos **itens 1 a 8**;

b) A repetição dos serviços pontuais e definitivos de instalação, configuração e treinamento previstos nos **itens 10 e 11**.

2.8. 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 o poder público, observadas as abrangências de aplicação.

CLÁUSULA TERCEIRA- MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS

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

CLÁUSULA QUARTA - SUBCONTRATAÇÃO

4.1. As regras sobre a subcontratação do objeto são aquelas estabelecidas no Termo de Referência, anexo a este Contrato.

CLÁUSULA QUINTA - PREÇO

5.1. O valor total da contratação é de R\$..... (.....).

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.

CLÁUSULA SEXTA - PAGAMENTO

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.

CLÁUSULA SÉTIMA - REAJUSTE

7.1. As regras acerca do reajuste do valor contratual são aquelas definidas no Termo de Referência, anexo a este Contrato.

CLÁUSULA OITAVA - OBRIGAÇÕES DO CONTRATANTE

8.1. São obrigações do Contratante, **além das previstas no item 5.1. termo de referência:**

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

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

8.4. Notificar o Contratado, por escrito, sobre vícios, defeitos, incorreções, imperfeições, falhas ou irregularidades verificadas na execução do objeto contratual, fixando prazo para que seja substituído, reparado ou corrigido, total ou parcialmente, às suas expensas, certificando-se de que as soluções por ele propostas sejam as mais adequadas;

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

8.6. 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;

8.7. Efetuar o pagamento ao Contratado do valor correspondente à execução do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência;

8.8. Aplicar ao Contratado as sanções previstas na lei e neste Contrato;

8.9. Não praticar atos de ingerência na administração do CONTRATADO, tais como:

8.9.1. indicar pessoas expressamente nominadas para executar direta ou indiretamente o objeto contratado;

8.9.2. fixar salário inferior ao definido em lei ou em ato normativo a ser pago pelo CONTRATADO;

8.9.3. estabelecer vínculo de subordinação com funcionário do CONTRATADO;

- 8.9.4. definir forma de pagamento mediante exclusivo reembolso dos salários pagos;
- 8.9.5. demandar a funcionário do CONTRATADO a execução de tarefas fora do escopo do objeto da contratação; e
- 8.9.6. prever exigências que constituam intervenção indevida da Administração na gestão interna do CONTRATADO.
- 8.10. Cientificar o órgão de representação judicial do CRM-MG para adoção das medidas cabíveis quando do descumprimento de obrigações pelo Contratado;
- 8.11. 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.
- 8.11.1. 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.
- 8.12. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo contratado no prazo máximo de 30 (trinta) dias.
- 8.13. Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.
- 8.14. 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.
- 8.15. 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.

CLÁUSULA NONA - OBRIGAÇÕES DO CONTRATADO

- 9.1. O Contratado deve cumprir todas as obrigações constantes deste Contrato e de 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, **além das previstas no item 5.2. do termo de referência:**
- 9.2. Atender às determinações regulares emitidas pelo fiscal ou gestor do contrato ou autoridade superior e prestar todo esclarecimento ou informação por eles solicitados;
- 9.3. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os bens e serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;
- 9.4. 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;
- 9.5. 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:
- 9.5.1. prova de regularidade relativa à Seguridade Social;
- 9.5.2. certidão conjunta relativa aos tributos federais e à Dívida Ativa da União;
- 9.5.3. certidões que comprovem a regularidade perante a Fazenda Municipal ou Distrital do

domicílio ou sede do CONTRATADO;

9.5.4. Certidão de Regularidade do FGTS – CRF; e

9.5.5. Certidão Negativa de Débitos Trabalhistas – CNDT.

9.6. 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, fiscais, comerciais e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao CONTRATANTE e não poderá onerar o objeto do contrato;

9.7. Comunicar ao Fiscal do contrato tempestivamente, observada a urgência da situação, qualquer ocorrência anormal ou acidente que se verifique no local da execução do objeto contratual, não ultrapassando o prazo de 24 (vinte e quatro) horas;

9.8. 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;

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

9.10. 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;

9.11. 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;

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

9.13. 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;

9.14. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do CONTRATANTE;

9.15. Alocar os empregados necessários ao perfeito cumprimento das cláusulas deste contrato, com habilitação e conhecimento adequados;

9.16. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos;

9.17. Fornecer todos os materiais, equipamentos, ferramentas e utensílios demandados, em quantidade, qualidade e tecnologia adequadas, com a observância às recomendações aceitas pela boa técnica, normas e legislação de regência;

9.18. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local de execução do objeto e nas melhores condições de segurança, higiene e disciplina;

9.19. 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;

9.20. Cumprir as normas de proteção ao trabalho, inclusive aquelas relativas à segurança e à saúde no trabalho;

9.21. Não submeter os trabalhadores a condições degradantes de trabalho, jornadas exaustivas, servidão por dívida ou trabalhos forçados;

9.22. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos de idade, exceto na condição de aprendiz para os maiores de quatorze anos de idade, observada a legislação pertinente;

9.23. Não submeter o menor de dezoito anos de idade à realização de trabalho noturno e em condições perigosas e insalubres e à realização de atividades constantes na Lista de Piores Formas de Trabalho Infantil, aprovada pelo Decreto nº 6.481, de 12 de junho de 2008;

9.24. Receber e dar o tratamento adequado a denúncias de discriminação, violência e assédio no ambiente de trabalho;

9.25. Manter preposto aceito pela Administração no local da obra ou do serviço para representá-lo na execução do contrato;

9.25.1. 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.

9.26. 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 de agente público que tenha desempenhado função na licitação ou que atue na fiscalização ou gestão do contrato, nos termos do art. 48, parágrafo único, da Lei nº 14.133, de 2021;

9.27. Prestar todo esclarecimento ou informação solicitada pelo CONTRATANTE ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do contrato;

9.28. Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência do contrato;

9.29. Assegurar aos seus trabalhadores ambiente de trabalho e instalações em condições adequadas ao cumprimento das normas de saúde, segurança e bem-estar no trabalho;

9.30. Fornecer equipamentos de proteção individual (EPI) e equipamentos de proteção coletiva (EPC), quando for o caso;

9.31. Garantir o acesso do CONTRATANTE, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do contrato;

9.32. Promover a organização técnica e administrativa dos serviços, de modo a conduzi-los eficaz e eficientemente, de acordo com os documentos e especificações que integram o Termo de Referência, no prazo determinado;

9.33. Instruir seus empregados quanto à necessidade de acatar as normas internas da Administração;

9.34. Instruir seus empregados a respeito das atividades a serem desempenhadas, alertando-os a não executar atividades não abrangidas pelo contrato, devendo o CONTRATADO relatar ao CONTRATANTE toda e qualquer ocorrência neste sentido, a fim de evitar desvio de função.

CLÁUSULA DÉCIMA - OBRIGAÇÕES PERTINENTES À LGPD

10.1. As partes deverão cumprir a Lei nº 13.709, de 14 de agosto de 2018 (LGPD), quanto a todos os dados pessoais a que tenham acesso em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.

10.2. Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu

acesso e de acordo com a boa-fé e com os princípios do art. 6º da LGPD.

10.3. É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei.

10.4. A Administração deverá ser informada no prazo de 5 (cinco) dias úteis sobre todos os contratos de suboperação firmados ou que venham a ser celebrados pelo Contratado.

10.5. Terminado o tratamento dos dados nos termos do art. 15 da LGPD, é dever do contratado eliminá-los, com exceção das hipóteses do art. 16 da LGPD, incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.

10.6. É dever do contratado orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.

10.7. O Contratado deverá exigir de suboperadores e subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.

10.8. O Contratante poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo o Contratado atender prontamente eventuais pedidos de comprovação formulados.

10.9. O Contratado deverá prestar, no prazo fixado pelo Contratante, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.

10.10. Bancos de dados formados a partir de contratos administrativos, notadamente aqueles que se proponham a armazenar dados pessoais, devem ser mantidos em ambiente virtual controlado, com registro individual rastreável de tratamentos realizados (LGPD, art. 37), com cada acesso, data, horário e registro da finalidade, para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.

10.10.1. Os referidos bancos de dados devem ser desenvolvidos em formato interoperável, a fim de garantir a reutilização desses dados pela Administração nas hipóteses previstas na LGPD.

10.11. O contrato está sujeito a ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a ANPD por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.

10.12. Os contratos e convênios de que trata o § 1º do art. 26 da LGPD deverão ser comunicados à autoridade nacional.

CLÁUSULA DÉCIMA PRIMEIRA - GARANTIA DE EXECUÇÃO

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

CLÁUSULA DÉCIMA SEGUNDA - INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

12.1. As regras acerca de infrações e sanções administrativas referentes à execução do contrato são aquelas definidas no Termo de Referência, anexo a este Contrato.

CLÁUSULA DÉCIMA TERCEIRA - DA EXTINÇÃO CONTRATUAL

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

13.2. 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.

13.3. 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.

13.4. 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.

13.5. O contrato poderá ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

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

13.5.2. 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.

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

13.6. O termo de extinção, sempre que possível, será precedido:

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

13.6.1.2. Relação dos pagamentos já efetuados e ainda devidos;

13.6.1.3. Indenizações e multas.

13.7. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório (art. 131, caput, da Lei n.º 14.133, de 2021).

13.8. O CONTRATANTE poderá ainda:

13.8.1. nos casos de obrigação de pagamento de multa pelo CONTRATADO, reter a garantia prestada a ser executada, conforme legislação que rege a matéria; e

13.8.2. nos casos em que houver necessidade de ressarcimento de prejuízos causados à Administração, nos termos do inciso IV do art. 139 da Lei n.º 14.133, de 2021, reter os eventuais créditos existentes em favor do CONTRATADO decorrentes do contrato.

13.9. 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).

CLÁUSULA DÉCIMA QUARTA - DOTAÇÃO ORÇAMENTÁRIA

14.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no orçamento do Conselho Regional de Medicina do Estado de Minas Gerais para o exercício de 2026, na dotação abaixo discriminada:

6.2.2.1.2.44.90.52.004 - EQUIPAMENTOS DE INFORMÁTICA

6.2.2.1.1.33.90.39.010 - MANUTENÇÃO DE SISTEMAS DE INFORMÁTICA - SOFTWARE

6.2.2.1.1.33.90.39.045 - AQUISIÇÃO DE SISTEMAS/PROGRAMAS (SOFTWARE) DE

INFORMÁTICA

6.2.2.1.1.33.90.39.025 - SERVIÇOS DE SELEÇÃO, TREINAMENTO E APERFEIÇOAMENTO

14.2. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

CLÁUSULA DÉCIMA QUINTA - DOS CASOS OMISSOS

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.

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

16.4. 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).

16.5. 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.

CLÁUSULA DÉCIMA SÉTIMA - PUBLICAÇÃO

17.1. Incumbirá ao contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo sítio oficial na Internet, em atenção ao art. 91, caput, da Lei n.º 14.133, de 2021, e ao art. 8º, §2º, da Lei n. 12.527, de 2011, c/c art. 7º, §3º, inciso V, do Decreto n. 7.724, de 2012.

CLÁUSULA DÉCIMA OITAVA - DO FORO

18.1. Fica eleito o Foro da Justiça Federal em Minas Gerais, Subseção Judiciária de Belo Horizonte, MG, para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não puderem ser compostos pela conciliação, conforme art. art. 92, §1º, da Lei nº 14.133/21.

Belo Horizonte, data de assinatura.

CONTRATANTE

CONSELHO REGIONAL DE MEDICINA DO ESTADO DE MINAS GERAIS

Cons. Ricardo Hernane Lacerda Gonçalves de Oliveira

Presidente do CRM-MG

CONTRATADO

Representante Legal

Testemunhas

1-

2-



Documento assinado eletronicamente por **Lívia Pinheiro de Azevedo**, **Coordenador(a) do Setor de Compras e Licitação do CRM-MG**, em 13/08/2026, às 15:51, com fundamento no art. 5º da [RESOLUÇÃO CFM nº2.308/2022, de 28 de março de 2022](#).



A autenticidade do documento pode ser conferida no site https://sei.cfm.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **4711084** e o código CRC **3A377576**.



Rua dos Timbiras, 1200 - Bairro Boa Viagem |
CEP 30140-064 | Belo Horizonte/MG -
<https://www.crmmg.org.br/>



Referência: Processo SEI nº 26.13.000003312-0 | data de inclusão: 13/08/2026