EDITAL DO PREGÃO, NA FORMA ELETRÔNICA, Nº 016/2024

PROCESSO ADMINISTRATIVO LICITATÓRIO ELETRÔNICO 016/2024

SISTEMA DE REGISTRO DE PREÇOS

O CONSÓRCIO INTERMUNICIPAL MULTIFINALITÁRIO DOS MUNICÍPIOS DO LAGO DE FURNAS CIMLAGO, Consórcio Público multifinalitário, com personalidade jurídica de direito público, inscrito no CNPJ sob o nº 50.387.580/000190, com sede na Rua Juscelino Barbosa, nº 816, centro em Alfenas, Estado de Minas Gerais – CEP 37.130-039, através de sua Pregoeira Oficial, Senhora Giuliana Menezes Matos, nomeada pela Portaria 002/2024, no uso de suas atribuições legais, na condição de ÓRGÃO GERENCIADOR, torna público e comunica aos interessados que realizará LICITAÇÃO COMPARTILHADA, na modalidade PREGÃO, NA FORMA ELETRÔNICA, auxiliado pelo SISTEMA DE REGISTRO DE PREÇOS para futura e eventual contratação, com fornecimento parcelado do objeto abaixo indicado para os ÓRGÃOS PARTICIPANTES desta licitação, observado as condições do edital e seus anexos que rege este pregão e aquelas enunciadas nas cláusulas que se seguem, nas disposições das Resoluções 004/2024 e 006/2024, bem como da Lei Federal n. 14.133, de 2021 e suas alterações.

TIPO: Menor preço GLOBAL

RECEBIMENTO DAS PROPOSTAS: Às 09h00mim, do dia 18/10/2024 até às 12:30mim do dia 31/10/2024.

DOCUMENTOS DE HABILITAÇÃO: Na mesma data e horário do recebimento das propostas.

ABERTURA E JULGAMENTO DAS PROPOSTAS: Às 13h30min do dia 31/10/2024.

INÍCIO DA SESSÃO DE DISPUTA DE PREÇOS: Às 13h40min do dia 31/10/2024.

REFERÊNCIA DE TEMPO: horário de Brasília (DF)

**PLATAFORMA ELETRÔNICA:** www.licitacimlago.com.br "Acesso Identificado "PLATAFORMA ELETRÔNICA: www.licitacimlago.com.br *"Acesso Identificado"*

Formalização de consultas/encaminhamentos:

Poderão ser formuladas consultas que deverão ser direcionadas única e exclusivamente de forma eletrônica, pelo sítio eletrônico www.licitacimlago.com.br ou pelo e-mail licita@cimlago.org.br.

## 1. DO OBJETO

1.1. O presente pregão tem como objeto o REGISTRO DE PREÇOS, por meio de licitação compartilhada, para a eventual e futura aquisição de infraestrutura como serviço, abrangendo soluções de armazenamento inteligente, proteção e armazenamento de dados, soluções de redes, proteção de perímetro, endpoint e gerenciamento de vulnerabilidades, com a finalidade de proporcionar ampla capacidade de atendimento aos usuários dos sistemas, incluindo serviços de instalação, configuração, transferência de conhecimento técnico e gerenciamento do ambiente, destinados a suprir futuras demandas, conforme especificações e condições estabelecidas no Anexo I e demais disposições do Edital, para atender os municípios consorciados ao Consórcio Intermunicipal Multifinalitário dos Municípios do Lago de Furnas – CIMLAGO, durante o prazo de validade da Ata de Registro de Preços:

1.2. O prazo de validade da Ata de Registro de Preços será **12 (doze) meses.**

1.3. O prazo de validade da Ata de Registro de Preços poderá ser prorrogado por igual período, desde que comprovada a vantajosidade do preço, nos termos do art. 84, caput, da Lei Federal n. 14.133, de 2021, e em conformidade com as disposições da Resolução 004/2024 do CIMLAGO.

1.4. O contrato ou documento equivalente decorrente da Ata de Registro de Preços terá sua vigência estabelecida conforme as disposições nela contidas.

1.5. O CIMLAGO é o Órgão Gerenciador responsável pela condução do conjunto de procedimentos para o registro de preços e pelo gerenciamento da Ata de Registro de Preços desta licitação compartilhada.

1.6. Os órgãos ou entidades da Administração Pública que não participaram dos procedimentos iniciais desta licitação e não integram a Ata de Registro de Preços poderão, na condição de "Órgão Não Participante", aderir à Ata de Registro de Preços, desde que atendidos os requisitos da Lei Federal nº 14.133/2021 e da Resolução 004/2024, nos termos e condições previstas neste Edital.

## 2. ÓRGÃOS PARTICIPANTES

2.1. São Órgãos Participantes do presente processo licitatório o Consórcio Intermunicipal Multifinalitário dos Municípios do Lago de Furnas – CIMLAGO e os órgãos consorciados ou referendados, conforme lista a seguir.

2.1.1. **Municípios:** Aguanil/MG, Alfenas/MG, Alpinópolis/MG, Alterosa/MG, Areado/MG, Boa Esperança/MG, Cabo Verde/MG, Camacho/MG, Campo do Meio/MG, Campos Gerais/MG, Cana Verde/MG, Candeias/MG, Capitólio/MG, Carmo do Rio Claro/MG, Conceição da Aparecida/MG, Coqueiral/MG, Cristais/MG, Divisa Nova/MG, Elói Mendes/MG, Fama/MG, Formiga/MG, Guapé/MG, Ilicínea/MG, Juruaia/MG, Lavras/MG, Machado/MG, Muzambinho/MG, Nepomuceno/MG, Paraguaçu/MG, Perdões/MG, Pimenta/MG, Poço Fundo/MG, Ribeirão Vermelho/MG, São João Batista do Glória/MG, São José da Barra/MG, Serrania/MG, Três Pontas/MG e Varginha/MG.

2.1.2. **Entidade Intermunicipal:** Consórcio Intermunicipal Multifinalitário dos Municípios do Lago de Furnas – CIMLAGO.

2.2. Entes da Federação consorciados: São os entes da federação que ratificaram por lei o Protocolo de Intenções do CIMLAGO e que participam dos procedimentos iniciais da licitação para o Sistema de Registro de Preços

2.3. Entes da Federação referendados: São os entes da federação consorciados ou identificados no Protocolo de Intenções do CIMLAGO, que poderão, a qualquer momento, ratificá-lo por lei, e que participam dos procedimentos iniciais da licitação para o Sistema de Registro de Preços.

2.4. Também são Órgãos Participantes os órgãos ou entidades dos Entes da Federação (União, Estado, Distrito Federal e Municípios), os Consórcios Públicos, as Associações de Municípios de Minas Gerais, que, após a assinatura de Convênio ou Termo de Cooperação Técnica com o CIMLAGO, poderão realizar contratações de produtos decorrentes deste processo administrativo licitatório, mediante solicitação e autorização do Órgão Gerenciador.

2.5. São Órgãos Não Participantes os órgãos ou entidades da Administração Pública que não participaram dos procedimentos iniciais da licitação e não integram a Ata de Registro de Preços, mas que, atendidos os requisitos da Lei Federal nº 14.133/2021, deste Edital e das Resoluções 004/2024 e 006/2024, podem aderir à Ata de Registro de Preços.

2.5.1. Desde que devidamente justificada a vantagem, a Ata de Registro de Preços, durante sua vigência, poderá ser utilizada por qualquer órgão ou entidade da administração pública dos Entes da Federação que não aderiram ao Projeto de Licitações Compartilhadas do CIMLAGO e/ou não tenham participado do certame licitatório e/ou não estejam previstos no edital como Órgãos Participantes, mediante anuência do Órgão Gerenciador.

2.5.2. Os órgãos e entidades que não participaram do registro de preços, quando desejarem fazer uso da Ata de Registro de Preços, deverão consultar o Órgão Gerenciador da ata para manifestação sobre a possibilidade de adesão.

2.5.3. A manifestação do Órgão Gerenciador, de que trata o item 2.5.2, fica condicionada à realização de estudo, pelos órgãos e entidades que não participaram do registro de preços, que demonstre o ganho de eficiência, a viabilidade e a economicidade para a administração pública na utilização da Ata de Registro de Preços, inclusive em situações de provável desabastecimento ou descontinuidade de serviço público.

2.5.4. Caberá ao fornecedor beneficiário da Ata de Registro de Preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento decorrente de adesão, desde que não prejudique as obrigações presentes e futuras decorrentes da ata, assumidas com o Órgão Gerenciador e Órgãos Participantes.

2.5.5. As aquisições ou contratações adicionais de que trata este artigo não poderão exceder, por órgão ou entidade, a 50% (cinquenta por cento) dos quantitativos dos itens do instrumento convocatório e registrados na Ata de Registro de Preços para o Órgão Gerenciador e para os Órgãos Participantes.

2.5.6. O quantitativo decorrente das adesões à Ata de Registro de Preços não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na Ata de Registro de Preços para o Órgão Gerenciador e para os Órgãos Participantes, independentemente do número de Órgãos Não Participantes que aderirem.

2.5.7. Após a autorização do Órgão Gerenciador para a utilização da Ata de Registro de Preços, o órgão não participante deverá efetivar a aquisição ou contratação solicitada em até 90 (noventa) dias, observado o prazo de vigência da ata.

2.5.8. Compete ao Órgão Não Participante a execução dos atos relativos à cobrança do cumprimento, pelo fornecedor, das obrigações contratualmente assumidas e a aplicação, observada a ampla defesa e o contraditório, de eventuais penalidades decorrentes do descumprimento de cláusulas contratuais, em relação às suas próprias contratações, informando as ocorrências ao Órgão Gerenciador.

2.5.9. É facultada aos órgãos ou entidades dos Entes da Federação a adesão à Ata de Registro de Preços do CIMLAGO decorrente do presente processo.

## 2.6. DA TARIFA ADMINISTRATIVA NAS ADESÕES DEFERIDAS:

2.6.1. A Lei Federal n° 11.107/2006, em seu Artigo 2°, § 2°, prevê que os consórcios públicos podem emitir documentos de cobrança e exercer atividades de arrecadação de tarifas e

outros preços públicos pela prestação de serviços ou pelo uso ou outorga de uso de bens públicos por eles administrados ou, mediante autorização específica, pelo ente da Federação consorciado.

2.6.2. A referida cobrança mencionada no item 2.6.1 está prevista no Estatuto Social vigente do CIMLAGO, em seu Art. 40, inc. I, letra G.

2.6.3. A questão está regulamentada pela **Resolução do CIMLAGO n° 006/2024**, que dispõe sobre a criação e aplicação da tarifa administrativa denominada **TARIFA ADMIN-LIC**, que incidirá sobre os serviços prestados e voltados para as adesões aos processos licitatórios, no percentual de 0,30% (zero vírgula trinta por cento) sobre o valor de cada adesão, a ser arcada pela empresa vencedora do certame. Esta tarifa destina-se a custear despesas tributárias e administrativas necessárias para garantir a continuidade dos serviços prestados pelo CIMLAGO.

**2.6.4. O inteiro teor da redação da Resolução 006/2024 encontra-se publicada no sítio: https://www.licitacimlago.com.br.**

## 3. DO CADASTRO DE RESERVA DE FORNECEDORES/ESTIMATIVA DE CONSUMO/REMANEJAMENTO

3.1. O Cadastro de Reserva de Fornecedores será formado por todos os licitantes classificados segundo a ordem da última proposta apresentada durante a fase competitiva, excetuados os classificados em primeiro lugar com os quais serão registrados Ata de Registro de Preços.

3.2. Os quantitativos estimados para consumo são formados pela demanda apresentada pelos Órgãos Participantes e Órgão Gerenciador. Esses quantitativos não vinculam qualquer obrigação do CIMLAGO ou Órgãos Participantes e não geram qualquer Direito ao Fornecedor.

3.3. Os Órgãos Participantes poderão adquirir de mais de um fornecedor registrado, segundo a ordem de classificação, desde que razões de interesse público justifiquem e que o

primeiro classificado não possua capacidade de fornecimento compatível com o solicitado.

3.4. As alterações dos quantitativos dos itens realizadas através do remanejamento interno entre os Órgãos Participantes não poderá causar acréscimo ou decréscimo nos valores dos itens iniciais previstas no processo licitatório.

3.5. Cabe ao Órgão Gerenciador controlar, autorizar e operar a realização do remanejamento dos quantitativos dos itens internamente entre os Órgãos Participantes.

## 4. DISPOSIÇÕES PRELIMINARES

4.1. O Pregão, na forma Eletrônica, será realizado em sessão pública, por meio da INTERNET, com condições de segurança criptografia e autenticação em todas as suas fases, através do Sistema de Pregão Eletrônico do Portal Oficial de Licitações do CIMLAGO.

4.2. A sessão eletrônica e todos os demais atos administrativos serão conduzidos pelo Consórcio Intermunicipal Multifinalitário dos Municípios do Lago de Furnas CIMLAGO, por intermédio de sua Pregoeira, mediante inserção e monitoramento de dados gerados ou transferidos para a plataforma digital disponível na página eletrônica do Portal Oficial de Licitações do CIMLAGO (www.licitacimlago.com.br).

## 5. RECEBIMENTO E ABERTURA DAS PROPOSTAS E DATA DO PREGÃO

5.1. O fornecedor deverá observar as datas e os horários limites previstos para a abertura da proposta, atentando também para a data e o horário de início da disputa, conforme indicado no site www.licitacimlago.com.br.

5.2. As propostas deverão ser cadastradas no sistema eletrônico (www.licitacimlago.com.br), podendo ser enviadas, substituídas ou excluídas até a data e hora previstas para o recebimento das propostas.

5.3. O acompanhamento do Sistema Eletrônico em todas as fases do presente Procedimento Administrativo é de responsabilidade do fornecedor.

## 6. CONDIÇÕES PARA PARTICIPAÇÃO

6.1. Poderão participar desta licitação todas as empresas ou sociedades, regularmente estabelecidas no País, que sejam especializadas e credenciadas no objeto desta licitação e que satisfaçam todas as exigências, especificações e normas contidas neste Edital, em seus anexos, e nos demais regramentos e normativas existentes no Brasil sobre a área de fornecimento.

6.2. Poderão participar deste Pregão Eletrônico as empresas que apresentarem toda a documentação exigida para o respectivo cadastramento junto ao Portal Oficial de Licitações do CIMLAGO.

6.3. Como requisito para participação no pregão, o licitante deverá, em campo próprio do sistema eletrônico, manifestar pleno conhecimento e atendimento às exigências de habilitação previstas no Edital.

6.4. **É vedada a participação de empresa em forma de consórcios ou grupos de empresas neste Processo Administrativo Licitatório.**

6.5. Não poderá participar da licitação a empresa que estiver sob falência, dissolução, liquidação, ou que tenha sido declarada inidônea pela Administração Pública, ou que estejam legalmente impedidas, ou ainda suspensa de participar de licitação. Também estão impedidas empresas controladoras, controladas ou coligadas, nos termos da Lei Federal n. 6.404, de 15 de dezembro de 1976, de concorrer entre si.

6.5. **O licitante deverá ter realizado a adesão ao Portal Oficial de Licitações do CIMLAGO, sendo sua a responsabilidade pela tramitação prévia nesse sentido.**

6.6. Não poderá participar da licitação pessoa física ou jurídica que, nos 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, devendo essa condição ser comprovada mediante declaração, conforme modelo constante deste edital (ANEXO V).

6.7. Não poderá participar da licitação quem 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 seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau. Essa condição deve ser comprovada mediante declaração, conforme modelo constante deste edital (ANEXO VI).

6.8. Não poderá participar da licitação pessoa física.

## 7. REGULAMENTO OPERACIONAL DO CERTAME

7.1. O certame será conduzido pela Pregoeira, com o auxílio da equipe de apoio, que terá, em especial, as seguintes atribuições:

a) Coordenar o processo licitatório;

b) Receber, analisar e decidir sobre as impugnações e os pedidos de esclarecimentos relativos ao edital, com o auxílio do responsável por sua elaboração, devendo tais manifestações ser apresentadas exclusivamente por meio do Portal de Compras do CIMLAGO (https://www.licitacimlago.com.br), dentro dos prazos legais e/ou previstos neste edital, sendo admitida, de forma subsidiária, a submissão por e-mail para licita@cimlago.org.br.

c) Conduzir a sessão pública por meio eletrônico;

d) Verificar a conformidade das propostas com os requisitos estabelecidos no instrumento convocatório;

e) Dirigir a etapa de lances;

f) Verificar e julgar as condições de habilitação dos licitantes;

g) Analisar a admissibilidade dos recursos interpostos, podendo, nesse caso, exercer o juízo de retratação no prazo de 03 (três) dias úteis (§ 2º do art. 165 da Lei Federal n. 14.133, de 2021), após o qual deverá encaminhar o recurso, devidamente instruído, para deliberação da autoridade competente;

h) Declarar o vencedor do certame;

i) Supervisionar os trabalhos da equipe de apoio;

j) Sanear erros ou falhas que não alterem a substância das propostas apresentadas;

k) Encaminhar à equipe de apoio os documentos de habilitação, caso seja possível sanar erros ou falhas que não comprometam a substância dos documentos e sua validade jurídica;

l) Encaminhar o processo, devidamente instruído, à autoridade competente, propondo a adjudicação, homologação e a elaboração das atas ou contratos administrativos correspondentes.

7.1.1. O(a) Pregoeiro(a) poderá solicitar manifestação técnica da assessoria jurídica ou de outros agentes públicos, de setores da entidade ou dos entes federados consorciados e/ou cooperados, a fim de subsidiar sua decisão.

CREDENCIAMENTO NO SISTEMA ELETRÔNICO:

7.2. Para acessar o sistema eletrônico, os interessados em participar do Pregão Eletrônico deverão obter, junto ao Portal Oficial de Licitações do CIMLAGO (https://www.licitacimlago.com.br), chave de identificação e senha pessoal, ambas intransferíveis e de exclusiva responsabilidade do Usuário.

7.3. A chave de identificação e a senha dos operadores poderão ser utilizadas em qualquer pregão eletrônico, salvo cancelamento por solicitação do Usuário ou por iniciativa do Portal Oficial de Licitações do CIMLAGO.

7.4. O sigilo da senha é de exclusiva responsabilidade do Usuário, assim como seu uso em

qualquer transação efetuada diretamente ou por meio de seu representante, não cabendo ao Portal Oficial de Licitações do CIMLAGO ou ao CIMLAGO a responsabilidade por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros.

7.5. O credenciamento do fornecedor e de seu representante legal junto ao sistema eletrônico implica a assunção de responsabilidade legal pelos atos praticados, a presunção de capacidade técnica para a realização das transações inerentes ao pregão eletrônico, bem como a aceitação das regras dos editais eletrônicos nos quais decidir participar.

PARTICIPAÇÃO

7.6. A participação no Pregão Eletrônico ocorrerá mediante a digitação da senha pessoal e intransferível do representante credenciado, seguida do envio da proposta de preços e dos documentos de habilitação exigidos no Edital, exclusivamente por meio do sistema eletrônico, observados os prazos e horários estabelecidos.

7.7. Compete ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do pregão, sendo responsável pelos prejuízos decorrentes da perda de oportunidades em razão da inobservância de mensagens emitidas pelo sistema ou por eventual desconexão.

7.8. A participação do licitante nesta licitação implica na aceitação de todos os termos deste Edital, obrigando o proponente vencedor à entrega dos itens nas condições, locais e prazos definidos.

PROPOSTA NO SISTEMA ELETRÔNICO

7.9. O encaminhamento de proposta e os documentos de habilitação exigidos no Edital, para o sistema eletrônico, pressupõe o pleno conhecimento e atendimento às exigências de habilitação e execução do Contrato previstas no Edital. O Licitante será responsável por todas as transações efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas, lances e aceitação das regras de cumprimento de suas obrigações.

7.10. No preenchimento da proposta eletrônica, deverão, obrigatoriamente, ser informadas no campo próprio as especificações, marcas/modelos, preços unitários e totais de todos os itens ofertados.

7.11. O objeto deverá estar totalmente e estritamente dentro das especificações contidas para os itens do Edital.

7.12. O licitante deverá encaminhar proposta, para o objeto deste Edital, exclusivamente por meio do sistema eletrônico, com os documentos de habilitação exigidos no Edital, até a data e horário indicados no preâmbulo deste Edital, quando então encerrar-se-á automaticamente a fase de recebimento de propostas.

7.13. A licitante deverá declarar, em campo próprio do sistema eletrônico, que cumpre plenamente os requisitos de habilitação e que sua proposta está em conformidade com as exigências do Edital.

7.14. A licitante enquadrada como microempresa ou empresa de pequeno porte deverá declarar, sob pena de decair seu Direito de Pequena Empresa, em campo próprio do Sistema, que atende aos requisitos do art. 3º da LC nº 123/06, para fazer jus aos benefícios previstos em lei.

7.15. A declaração falsa relativa ao cumprimento dos requisitos de habilitação, à conformidade da proposta ou ao enquadramento como microempresa ou empresa de pequeno porte sujeitará a licitante às sanções previstas neste Edital.

7.16. As propostas ficarão disponíveis no sistema eletrônico após a sua liberação para todos.

7.17. Qualquer elemento que possa identificar a licitante importa na desclassificação da proposta, sem prejuízo das sanções previstas neste Edital.

7.18. Até a data limite para a apresentação da proposta, a licitante poderá retirar ou substituir a proposta e os documentos de habilitação anteriormente encaminhados. Após a data limite, não poderá haver desistência da proposta, salvo aceitação de justificativa pelo

CIMLAGO, podendo ocorrer o complemento dos documentos de habilitação e regularidade fiscal após a fase de lances, se for declarado vencedor, no prazo estipulado pelo(a) Pregoeiro(a), não inferior a 02 (duas) horas.

7.19. Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados para avaliação do(a) Pregoeiro(a) e para acesso público após o encerramento do envio de lances.

7.20. O prazo de validade da proposta de preços não poderá ser inferior a 90 (noventa) dias, contados da abertura das propostas virtuais.

7.21. Nos preços propostos deverão estar incluídos todos os custos diretos e indiretos necessários à perfeita execução do objeto, como entregas nos municípios consorciados, encargos sociais e inclusive as despesas com materiais e/ou equipamentos fornecidos, mão de obra especializada ou não, fretes, seguros em geral, equipamentos auxiliares, ferramentas, encargos da Legislação Tributária, Social, Trabalhista e Previdenciária, da infortunística do trabalho e responsabilidade civil por quaisquer danos causados a terceiros ou dispêndios resultantes de impostos, taxas, regulamentos e posturas municipais, estaduais e federais, enfim, tudo o que for necessário para a execução total e completa do objeto desta licitação.

7.22. Para composição do preço unitário e total do item, os participantes deverão considerar até 02 (dois) dígitos após a vírgula. No fornecimento posterior, a totalização do pedido contabilizado (total da Nota Fiscal) será de dois dígitos após a vírgula. Se houver algum dígito a mais, não importa a quantidade, será desconsiderado.

7.23. A apresentação de proposta implica no compromisso, por parte do licitante, com o cumprimento dos respectivos métodos de controle de qualidade e da sistemática de certificação de conformidade de cada item.

## 8. ABERTURA DAS PROPOSTAS E FORMULAÇÃO DOS LANCES

8.1. A partir do horário previsto no Edital e no site www.licitacimlago.com.br, terá início a

sessão pública do pregão, na forma eletrônica, com a divulgação das propostas de preços recebidas, momento em que o(a) Pregoeiro(a) passará a avaliar a aceitabilidade das propostas.

8.2. Serão analisadas as propostas apresentadas, sendo desclassificadas, com a devida motivação, aquelas que não estiverem em conformidade com os requisitos estabelecidos neste Edital.

8.2.1. Serão desclassificadas as propostas que não especificarem a marca/modelo dos itens (quando necessário) ou que estiverem em desacordo com as marcas/modelos constantes do "*cadastro de bens pré-qualificados do CIMLAGO*".

8.3. Somente as licitantes com propostas classificadas participarão da fase de lances.

8.4. Todas as propostas classificadas serão consideradas como lances na fase de disputas e serão ordenadas por valor, de forma decrescente.

8.5. Aberta a etapa competitiva, os representantes dos fornecedores deverão estar conectados ao sistema para participar da sessão de lances. A cada lance ofertado, o participante será imediatamente informado sobre seu recebimento, horário de registro e valor, mantendo-se em sigilo a identificação de todos os demais ofertantes.

8.6. Durante a sessão pública, a comunicação entre o(a) Pregoeiro(a) e as licitantes ocorrerá exclusivamente mediante troca de mensagens, em campo próprio do sistema eletrônico.

8.7. Os itens poderão ser disponibilizados por grupo, para otimização dos trabalhos do(a) Pregoeiro(a) e da Equipe de Apoio, podendo a disputa de lances se estender para outros dias, se necessário.

8.8. Poderão ser ofertados lances intermediários, na impossibilidade de cobrir o menor preço, desde que sejam inferiores ao último lance ofertado pelo próprio licitante e diferentes de qualquer lance válido para o item.

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

8.10. O intervalo mínimo de diferença de valores ou percentuais entre os lances, tanto em relação aos lances intermediários quanto à proposta que cobrir a melhor oferta, deverá ser de no mínimo de R$ 500,00 (quinhentos reais).

8.11. Fica a critério do(a) Pregoeiro(a) a autorização para correção de lances com valores digitados erroneamente ou em situações semelhantes.

8.12. No caso de desconexão do(a) Pregoeiro(a) durante a etapa competitiva do Pregão, na forma eletrônica, o sistema eletrônico poderá permanecer acessível às licitantes para a recepção dos lances, retornando o(a) Pregoeiro(a) à sua atuação no certame tão logo seja possível, sem prejuízo dos atos realizados.

8.13. Quando a desconexão persistir por tempo superior a 10 (dez) minutos, a sessão do Pregão, na forma eletrônica, será SUSPENSA, tendo seu reinício somente após comunicação expressa aos operadores representantes dos participantes, por meio de mensagem eletrônica (e-mail) informando a data e hora da reabertura da sessão.

8.14. SERÁ DESCLASSIFICADA A PROPOSTA VENDEDORA QUE:

8.14.1. Contiver vícios insanáveis.

8.14.2. Não observar as especificações técnicas estabelecidas no Termo de Referência.

8.14.3. Apresentar preços inexequíveis ou permanecer acima do preço máximo definido para a contratação.

8.14.4. Não tiver sua exequibilidade demonstrada, quando exigido pela Administração.

8.14.5. Apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.

8.14.6. No caso de bens e serviços em geral, SERÁ INDÍCIO DE INEXEQUIBILIDADE das propostas a apresentação de valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração.

8.14.7. A inexequibilidade, na hipótese de que trata o item 8.14.6, somente será considerada após diligência do(a) Pregoeiro(a), que comprove:

a) Que o custo do licitante ultrapassa o valor da proposta; e

b) A inexistência de custos de oportunidade capazes de justificar o valor ofertado.

8.14.8. Em contratações de serviços de engenharia, além das disposições acima, a análise de exequibilidade e sobrepreço considerará o seguinte:

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

b) No regime de empreitada por preço unitário, a caracterização do sobrepreço se dará pela superação do valor global estimado e pela superação de custo unitário considerado relevante, conforme planilha anexa ao edital, quando for o caso;

c) No caso de 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.

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

8.14.10 O fornecedor que não cotar todos os itens do lote será desclassificado.

(MODO DE DISPUTA ABERTO)

8.15. No pregão eletrônico, será adotado o modo de disputa "*aberto*", no qual os licitantes apresentarão lances públicos e sucessivos, com possibilidade de prorrogações automáticas.

8.16. A etapa de lances da sessão pública terá uma duração inicial de **10 (dez) minutos**. Após esse período, a sessão será prorrogada automaticamente pelo sistema sempre que um lance for ofertado nos últimos **2 (dois) minutos**.

8.17. Essa prorrogação, com duração de **2 (dois) minutos**, ocorrerá sucessivamente sempre que novos lances forem registrados dentro desse período, inclusive no caso de lances intermediários.

8.18. Se não houver novos lances conforme estabelecido, a sessão pública será automaticamente encerrada.

8.19. No entanto, caso a fase competitiva se encerre sem prorrogação automática, o(a) Pregoeiro(a) (a), assessorado pela equipe de apoio, poderá, justificadamente, decidir pelo reinício da sessão pública de lances para buscar a obtenção do melhor preço.

8.20. O sistema informará a proposta de menor preço imediatamente após o encerramento da etapa de lances ou, quando necessário, após negociação e decisão do(a) Pregoeiro(a) acerca da aceitação do lance de menor valor.

8.21. O não cumprimento do envio dos documentos de habilitação exigidos no Edital, dentro do prazo fixado, resultará nas sanções previstas, podendo o(a) Pregoeiro(a) convocar a empresa que apresentou a proposta ou o lance subsequente.

8.22. Se a proposta ou o lance de menor valor não for aceitável, ou se o fornecedor não cumprir as exigências habilitatórias, o(a) Pregoeiro(a) examinará a proposta ou o lance subsequente, verificando sua compatibilidade e a habilitação do participante conforme a ordem de classificação. Este processo será repetido até que se encontre uma proposta ou lance que atenda às exigências do Edital. Nesse momento, o(a) Pregoeiro(a) também poderá negociar com o participante para obter um preço mais vantajoso.

8.23. Caso não sejam apresentados lances, será verificada a conformidade entre a proposta de menor preço e o valor estimado para a contratação.

8.24. O(a) Pregoeiro(a) poderá convocar o licitante para enviar documentos complementares de forma digital, por meio da funcionalidade disponível no sistema, com um prazo mínimo de 2 (duas) horas, sob pena de não aceitação da proposta.

8.24.1. Esse prazo poderá ser prorrogado pelo(a) Pregoeiro(a) mediante solicitação escrita e justificada do licitante, desde que formulada antes do fim do prazo original e formalmente aceita.

8.24.2. Entre os documentos que podem ser solicitados como complementares, destacam-se aqueles que detalham as características do material ofertado, como marca, modelo, tipo, fabricante e procedência, além de outras informações pertinentes, como catálogos, folhetos ou propostas. Esses documentos devem ser encaminhados por meio eletrônico ou por outro meio indicado pelo(a) Pregoeiro(a), sem prejuízo de posterior envio pelo sistema eletrônico, sob pena de não aceitação da proposta. Também poderá ser solicitada a complementação dos documentos de habilitação e regularidade fiscal após a etapa de lances.

8.25. Uma vez constatado que todas as exigências do Edital foram cumpridas e não havendo interposição de recursos, o objeto será adjudicado ao autor da proposta ou lance de menor preço que tenha sido habilitado.

8.26. No caso de empate, conforme estabelecem os artigos 44 e 45 da Lei Complementar 123/2006, o(a) Pregoeiro(a) aplicará os critérios de desempate em favor das microempresas e empresas de pequeno porte, desde que o fornecedor tenha declarado essa condição no cadastramento junto ao Portal Oficial de Licitações do CIMLAGO. Após o desempate, o(a) Pregoeiro(a) poderá negociar um melhor preço caso a empresa vencedora não atinja o valor de referência definido pela administração pública. Se a empresa aceitar reduzir o preço ao valor estimado, será declarada vencedora do pregão; caso contrário, a negociação poderá continuar com as empresas subsequentes.

8.26.1. O tratamento diferenciado previsto na Lei Complementar 123/2006 não será concedido nos itens cujo valor estimado for superior à receita bruta máxima permitida para o enquadramento como empresa de pequeno porte. Também não será aplicado a empresas que, no ano da licitação, tenham celebrado contratos com a Administração Pública que, somados, ultrapassem a receita bruta máxima permitida para esse enquadramento, conforme disposto no artigo 4º, § 1º, inciso I, e § 2º, da Lei Federal 14.133/2021.

8.27. Persistindo o empate, serão utilizados os critérios previstos no artigo 60 da Lei Federal 14.133/2021.

## 9. PROPOSTA ESCRITA E FORNECIMENTO

9.1. A empresa vencedora deverá enviar ao Pregoeiro, via sistema, a Proposta de Preços ajustada ao último lance ofertado, após a negociação, no prazo mínimo de duas horas. Essa proposta deverá ser acompanhada, quando necessário, dos documentos complementares que confirmem aqueles já exigidos e apresentados conforme o Edital.

9.2. O prazo para a apresentação da proposta final poderá ser prorrogado, desde que devidamente justificado e a critério do Pregoeiro.

### NA PROPOSTA ESCRITA, DEVERÁ CONTER:

a) A proposta deve conter o nome do proponente, endereço, identificação (individual ou social), número do CNPJ e da Inscrição Estadual, telefone, fax e e-mail de contato.

b) Todas as folhas da proposta devem estar datadas, assinadas e rubricadas pelo representante legal do proponente, podendo ser de forma digital, desde que cumpridos os requisitos legais.

c) Nos preços propostos devem estar incluídos todos os custos diretos e indiretos necessários para a perfeita execução do objeto, incluindo entregas nos municípios consorciados, encargos sociais e despesas com materiais e/ou equipamentos fornecidos, mão de obra especializada ou não, fretes, seguros em geral, equipamentos auxiliares, ferramentas,

encargos da Legislação Tributária, Social, Trabalhista e Previdenciária, despesas relacionadas à segurança no trabalho e responsabilidade civil por quaisquer danos causados a terceiros, além de impostos, taxas, regulamentos e posturas municipais, estaduais e federais, ou seja, todos os custos necessários para a execução total e completa do objeto desta licitação.

d) O prazo de validade da proposta de preços deve ser de, no mínimo, **90 (noventa) dias**, contados a partir da abertura das propostas virtuais.

e) Os preços dos **itens devem ser discriminados em moeda corrente nacional**, limitados a **2 (duas)** casas decimais para os centavos.

f) A proposta deve indicar que o prazo de validade da Ata de Registro de Preços é de **12 (doze) meses**, com possibilidade de prorrogação por igual período.

g) **O prazo de entrega dos itens observará rigorosamente os prazos estabelecidos no Anexo I – Termo de Referência.**

h) A especificação completa da marca/modelo do produto oferecido deve estar de acordo com as informações apresentadas na Proposta Eletrônica, contendo dados técnicos que permitam sua completa avaliação, em **TOTAL CONFORMIDADE** com o item 1.1 deste Edital.

i) A proposta deve incluir o valor unitário e o valor total com a quantidade estimada dos itens.

j) Devem ser fornecidos os dados bancários, dados do representante legal, declaração de domicílio eletrônico e declaração de assinatura por certificação digital, conforme modelo especificado no **ANEXO III**.

## 10. GARANTIA

10.1. Não será exigida a prestação de garantia para o presente processo.

## 11. DAS AMOSTRAS

11.1. Não haverá exigência de apresentação de amostras neste processo.

## 12. DA HABILITAÇÃO

12.1. Toda a documentação de habilitação deverá ser encaminhada juntamente com a proposta de preços, conforme previsto neste Edital, em formato digital e exclusivamente por meio do sistema.

12.1.2. O Pregoeiro poderá realizar a verificação tanto em nome da empresa licitante quanto em nome de seu sócio majoritário, mediante consulta aos seguintes cadastros, a fim de identificar se há alguma restrição:

I. Sistema de Cadastramento Unificado de Fornecedores – SICAF;

II. Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/ceis);

III. Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/cnep);

IV. Para licitantes pessoa jurídica, poderá haver a substituição das consultas dos itens II e III pela Consulta Consolidada de Pessoa Jurídica do TCU (https://certidoes-apf.apps.tcu.gov.br/).

12.1.3. Constatada a existência de sanção, o licitante será considerado inabilitado, por ausência de condições de participação.

12.2. Para a habilitação nesta licitação, será exigido o envio, através do sistema, dos documentos listados conforme a relação estabelecida a seguir:

### 12.2.1. PARA COMPROVAR A HABILITAÇÃO JURÍDICA:

11.2.1.1. Registro comercial, no caso de empresa individual;

11.2.1.2. Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial, no caso de sociedades empresárias. Para sociedades por ações, é necessário

apresentar os documentos de eleição de seus administradores;

11.2.1.3 Inscrição do ato constitutivo, no caso de sociedades simples, acompanhada de prova da diretoria em exercício;

11.2.1.4 Decreto de autorização, no caso de empresa ou sociedade estrangeira em funcionamento no País, bem como o ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando exigido pelas atividades desempenhadas;

11.2.1.5 No caso de Microempreendedor Individual (MEI), é necessário apresentar o Certificado da Condição de Microempreendedor Individual (CCMEI), cuja aceitação estará condicionada à verificação da autenticidade no portal www.portaldoempreendedor.gov.br.

11.2.1.6 Para sociedade empresária ou empresa individual de responsabilidade limitada (EIRELI), é necessário apresentar o ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores.

11.2.1.7. No caso de cooperativa, é necessário apresentar a ata de fundação e o estatuto social em vigor, juntamente com a ata da assembleia que o aprovou, devidamente arquivados na Junta Comercial ou inscritos no Registro Civil das Pessoas Jurídicas da respectiva sede, bem como o registro previsto no art. 107 da Lei nº 5.764, de 1971.

Observação: Todos os documentos mencionados devem ser acompanhados de todas as alterações ou da consolidação respectiva.

12.2.2. PARA COMPROVAR A REGULARIDADE FISCAL E TRABALHISTA:

12.2.2.1. Prova de inscrição no Cadastro Nacional de Pessoa Jurídica (CNPJ/MF);

12.2.2.2. Prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, referente à sede ou domicílio do(a) licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

12.2.2.3. Prova de regularidade com a Fazenda Municipal do domicílio ou sede do(a) licitante, mediante apresentação de certidão negativa ou positiva com efeitos de negativa, emitida pela secretaria competente do município;

12.2.2.4. Prova de regularidade com a Fazenda Estadual do domicílio ou sede do(a) licitante, mediante apresentação de certidão negativa ou positiva com efeitos de negativa, emitida pela secretaria competente do estado;

12.2.2.5. Prova de regularidade com a Fazenda Federal e a Seguridade Social, mediante apresentação de Certidão Negativa de Débitos Relativos a Créditos Tributários Federais e à Dívida Ativa da União, ou Certidão Positiva com Efeitos de Negativa, emitida pela Secretaria da Receita Federal do Brasil ou pela Procuradoria-Geral da Fazenda Nacional;

12.2.2.6. Prova de regularidade de débito para com o Fundo de Garantia por Tempo de Serviço (FGTS);

12.2.2.7. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeitos 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 (CNDT expedida pelo Tribunal Superior do Trabalho na internet, http://www.tst.jus.br, de acordo com a Lei nº 12.440/11, de 7 de julho de 2011).

12.2.2.8. Serão aceitas certidões positivas com efeitos de negativa.

12.2.2.9. No caso de licitantes classificadas como Microempresa (ME) ou Empresa de Pequeno Porte (EPP), será exigida a apresentação de documentação comprobatória de sua regularidade fiscal. Contudo, caso seja verificada alguma restrição, impropriedade ou pendência exclusivamente referente a essa documentação, será concedido o prazo de 5 (cinco) dias úteis para a regularização, contados a partir da declaração de vencedora e da preclusão do direito de interposição de recurso. Esse prazo poderá ser prorrogado por igual período, a critério da Administração, conforme previsto na Lei Complementar nº 123/06.

12.2.3. PARA COMPROVAR A QUALIFICAÇÃO ECONÔMICO-FINANCEIRA:

12.2.3.1. Certidão Negativa de Falência, Concordata e Recuperação Judicial ou Extrajudicial, expedida pelo distribuidor competente da localidade da sede da pessoa jurídica, conforme o disposto no art. 69, caput, inciso II, da Lei nº 14.133/2021, emitida no prazo máximo de 60 (sessenta) dias antes da data estabelecida para a entrega das propostas.

12.2.3.2. Balanço Patrimonial, Demonstração de Resultado do Exercício e demais demonstrações contábeis referentes ao último exercício social encerrado, comprovando:

I. Índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um).

12.2.3.3. A capacidade financeira da sociedade empresária será avaliada com base nos seguintes indicadores, cujas fórmulas de cálculo estão abaixo descritas:

a) **Índice de Liquidez Geral (ILG):** Avalia a solvência da empresa no curto e no longo prazo, indicando a capacidade de cumprir suas obrigações, considerando os recursos disponíveis e realizáveis a curto prazo.

$$ILG = \frac{\text{Ativo Circulante + Realizável a Longo Prazo}}{\text{Passivo Circulante + Exigível a Longo Prazo}} = \text{ou} > 1{,}00.$$

b) **Índice de Liquidez Corrente (ILC):** Avalia a solvência no curto prazo, verificando a capacidade da empresa de liquidar suas obrigações de curto prazo com os recursos disponíveis no mesmo período.

$$ILC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}} = \text{ou} > 1{,}00.$$

c) **Índice de Endividamento Geral (IGE):** Avalia o nível de endividamento da empresa, comparando o capital de terceiros com os recursos próprios.

$$IGE = \frac{\text{PASSIVO CIRCULANTE + PASSIVO EXIGÍVEL A LONGO PRAZO}}{\text{ATIVO TOTAL}} = \text{ou} < 0{,}50.$$

**Nota 1:** Em conformidade com o disposto no §1º do artigo 69 da Lei nº 14.133/2021, os indicadores referidos neste item deverão ser calculados pela própria empresa e confirmados pelo responsável contábil, mediante assinatura e indicação de seu nome e número de registro no Conselho Regional de Contabilidade (CRC).

12.2.3.4. Os documentos mencionados acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital (ECD) ao SPED.

c.2.) As empresas que não atenderem em qualquer dos índices, deverão comprovar que possuem patrimônio líquido mínimo de 10% (dez por cento) do valor estimado para os primeiros 12 (doze) meses.

12.2.3.5. As empresas constituídas no exercício financeiro da licitação deverão atender a todas as exigências de habilitação, podendo substituir os demonstrativos contábeis pelo balanço de abertura, devidamente assinados por profissional legalmente habilitado e pelo representante legal da empresa, registrados na Junta Comercial competente, conforme o art. 65, §1º, da Lei nº 14.133, de 2021.

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

12.2.3.7. No caso de Sociedades Anônimas, deve-se apresentar a publicação em Diário Oficial ou em jornal de grande circulação, acompanhada das respectivas demonstrações de conta de resultados. Para sociedades civis, o balanço e as demonstrações contábeis devem ser apresentados conforme a legislação civil aplicável.

12.2.3.8. Os tipos societários não sujeitos à Escrituração Contábil Digital (ECD) deverão apresentar cópias autenticadas do Balanço Patrimonial e das Demonstrações Contábeis, devidamente registrados na Junta Comercial do estado sede da licitante, incluindo cópias das folhas do Livro Diário, contendo os termos de abertura e encerramento, devidamente assinados pelo representante legal da empresa e por profissional de contabilidade habilitado, sendo vedada a substituição por balancetes ou balanços provisórios. Tais documentos poderão ser atualizados por índices oficiais, desde que encerrados há mais de 3 (três) meses da data de apresentação da proposta.

12.2.3.9. Os tipos societários obrigados à Escrituração Contábil Digital (ECD), conforme as disposições do Decreto nº 6.022/2007, regulamentado pela IN RFB nº 1420/2013 e suas alterações, além da IN nº 109/2008 do DNRC, deverão apresentar cópias autenticadas do Balanço Patrimonial e das Demonstrações Contábeis, assinados tempestivamente pelo representante legal da empresa e por profissional de contabilidade habilitado, sendo vedada a substituição por balancetes ou balanços provisórios. Esses documentos poderão ser atualizados por índices oficiais se encerrados há mais de 3 (três) meses da data de apresentação da proposta, devendo ser acompanhados dos seguintes documentos relativos ao último exercício social encerrado:

a) Cópia do Recibo de Entrega de Livro Digital transmitido via Sistema Público de Escrituração Digital (SPED);

b) Cópias dos Termos de Abertura e Encerramento do Livro Diário Digital extraídos do SPED;

c) Cópias do Balanço e da Demonstração do Resultado do Exercício extraídos do SPED.

### 12.2.4. DEMAIS DOCUMENTOS PARA COMPROVAR A HABILITAÇÃO – DECLARAÇÕES:

12.2.4.1 Declaração de Pleno Atendimento aos Requisitos de Habilitação, podendo ser utilizado o modelo do Anexo IV deste Edital;

12.2.4.2 Declaração de que a empresa não está declarada inidônea para licitar e contratar com a Administração Pública, nem suspensa do direito de licitar ou contratar com o CIMLAGO, podendo ser utilizado o modelo do Anexo V deste Edital;

12.2.4.3 Declaração de que a empresa não emprega trabalhadores menores de 18 anos em atividades noturnas, perigosas ou insalubres, nem menores de 16 anos em qualquer trabalho, salvo na condição de aprendiz a partir dos 14 anos, conforme a legislação vigente, podendo ser utilizado o modelo do Anexo IX deste Edital;

12.2.4.4 Declaração atestando que a empresa licitante não possui em seu quadro societário servidor público ativo, empregado de empresa pública ou de sociedade de economia mista, podendo ser utilizado o modelo do Anexo VI deste Edital;

12.2.4.5 Declaração de Enquadramento como Microempresa (ME) ou Empresa de Pequeno Porte (EPP), podendo ser utilizado o modelo do Anexo VIII. A presente declaração não dispensa a obrigação do licitante de assinalar a opção no campo correspondente do Sistema no momento do credenciamento e da apresentação da documentação para participação no certame;

12.2.4.6 Declaração de Enquadramento de Receita Bruta, podendo ser utilizado o modelo do Anexo VIII deste Edital;

12.2.4.7 Declaração de cumprimento do Art. 7°, inciso XXXIII, da Constituição da República Federativa do Brasil, podendo ser utilizado o modelo do Anexo IX deste Edital;

12.2.4.8 Declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitados da Previdência Social, podendo ser utilizado o modelo do Anexo X deste Edital;

12.2.4.9 O objeto social descrito no ato constitutivo referente ao item (12.2.1.2.) deve possuir ramo de atividade compatível com o objeto licitado.

12.2.4.10 Qualquer informação incompleta ou inverídica contida nos documentos apresentados, apurada pelo(a) Pregoeiro(a) mediante simples conferência ou diligência, implicará na inabilitação do(a) respectivo(a) licitante e no envio dos documentos ao Ministério Público de Minas Gerais (MP/MG.) para apuração de eventual prática delituosa.

12.2.4.11 Não serão aceitos protocolos de pedidos ou solicitações de documentos em substituição aos documentos requeridos no presente Edital.

12.2.4.12 A existência de restrição quanto à regularidade fiscal e trabalhista não impede que o(a) licitante qualificado(a) como microempresa ou empresa de pequeno porte seja declarado(a) vencedor(a), desde que atenda a todas as demais exigências do edital.

12.2.4.13 A declaração do vencedor ocorrerá no momento imediatamente posterior à fase de habilitação.

12.2.4.14 Havendo restrição quanto à regularidade fiscal ou trabalhista no caso de microempresa, empresa de pequeno porte ou microempreendedor equiparado, será concedido um prazo de 5 (cinco) dias úteis para sua regularização, prorrogável por igual período mediante justificativa tempestiva e aceita pelo(a) Pregoeiro(a) e equipe de apoio, conforme os termos da Lei Complementar nº 147, de 07 de agosto de 2014.

12.2.4.15 A não regularização fiscal e trabalhista no prazo previsto no subitem anterior acarretará a inabilitação do(a) licitante, sem prejuízo das sanções previstas neste Edital, sendo facultada a convocação dos(as) licitantes remanescentes, na ordem de classificação. Se, na ordem de classificação, houver outra microempresa, empresa de pequeno porte ou equiparada com alguma restrição na documentação fiscal e trabalhista, será concedido o mesmo prazo para regularização.

12.2.4.16 Havendo necessidade de análise minuciosa dos documentos exigidos, o(a)

Pregoeiro(a) suspenderá a sessão, informando no "*chat*" a nova data e horário para sua continuidade.

12.2.4.17 Será inabilitado(a) o(a) licitante que não comprovar sua habilitação, seja por não apresentar quaisquer dos documentos exigidos, seja por apresentá-los em desacordo com o estabelecido neste Edital.

12.2.4.18 Constatado o atendimento às exigências de habilitação fixadas no Edital, o(a) licitante será declarado(a) vencedor(a).

12.2.4.19 **As certidões que não possuírem prazo de validade serão aceitas apenas se emitidas há no máximo 90 (noventa) dias consecutivos antes da data de abertura da sessão deste Pregão**.

12.2.4.20 Na hipótese de a proposta vencedora não ser aceitável ou de o(a) licitante não atender às exigências para habilitação, o(a) Pregoeiro(a) examinará a proposta subsequente e, assim, sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao Edital.

## 12.2.5. PARA COMPROVAR A DA QUALIFICAÇÃO TÉCNICA

12.2.5.1. Atestado(s) de Capacidade Técnica que comprove(m) o fornecimento de solução de armazenamento inteligente ou de hiperconvergência de natureza idêntica ou similar à presente licitação, expedido por pessoa jurídica de direito público ou privado, que comprove a aptidão da licitante para o desempenho do objeto licitado.

12.2.5.2. Atestado(s) de Capacidade Técnica que comprove(m) o fornecimento de solução de redes de natureza idêntica ou similar à presente licitação, expedido por pessoa jurídica de direito público ou privado, que comprove a aptidão da licitante para o desempenho do objeto licitado.

12.2.5.3. Atestado(s) de Capacidade Técnica que comprove(m) o fornecimento de solução de proteção de dados de natureza idêntica ou similar à presente licitação, expedido por pessoa

jurídica de direito público ou privado, que comprove a aptidão da licitante para o desempenho do objeto licitado.

12.2.5.4. Atestado(s) de Capacidade Técnica que comprove(m) o fornecimento de solução de armazenamento de dados de natureza idêntica ou similar à presente licitação, expedido por pessoa jurídica de direito público ou privado, que comprove a aptidão da licitante para o desempenho do objeto licitado.

12.2.5.5. Atestado(s) de Capacidade Técnica que comprove(m) o fornecimento de soluções e serviços de Next Generation Firewall e suas respectivas características, com suporte, garantia e instalação.

12.2.5.6. Atestado(s) de Capacidade Técnica que comprove(m) o fornecimento de soluções e serviços de Solução de Endpoint Protection (XDR ou EDR) e suas respectivas características, com suporte, garantia e instalação.

12.2.5.7. Atestado(s) de Capacidade Técnica que comprove(m) o fornecimento de soluções e serviços de Análise de Vulnerabilidades e suas respectivas características, com suporte, garantia e instalação.

12.2.5.8. Atestado(s) de Capacidade Técnica que comprove(m) o fornecimento de serviços de segurança da informação por meio de Centro de Operações de Segurança (CSOC) 24x7.

12.2.5.9. Atestado(s) de Capacidade Técnica que comprove(m) o fornecimento de serviços de resposta a incidentes.

12.2.5.10. Será admitida a soma de atestados de capacidade técnica para comprovação da prestação dos serviços e fornecimento das soluções solicitados.

12.2.5.10.1. Mediante solicitação da contratante, a licitante deverá informar os dados de contato do(s) emitente(s) do(s) Atestado(s), tais como telefone, endereço e e-mail.

12.2.5.11. Caso a contratante julgue necessário, poderão ser solicitadas cópias dos contratos, aditivos da prestação dos respectivos serviços e fornecimentos, além das Notas Fiscais correspondentes aos Atestados apresentados, uma vez que poderão ser objeto de diligências para verificação da autenticidade de seu conteúdo.

12.2.5.12. No caso de Atestados emitidos por empresas da iniciativa privada, não serão aceitos aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da proponente. Serão consideradas pertencentes ao mesmo grupo empresarial as empresas controladas ou controladoras da proponente, ou aquelas em que haja, no mínimo, uma pessoa física ou jurídica em comum no quadro societário.

12.2.5.13. Atestados emitidos por empresas do mesmo grupo empresarial, contemplando os mesmos objetos no mesmo período, serão considerados como um único atestado, sendo computado o de maior volume.

12.2.5.14. Deverá ser apresentada declaração do(s) fabricante(s), atestando que a licitante faz parte de sua rede de parceiros, estando apta a fornecer, instalar e prestar os serviços descritos no edital.

12.2.5.15. A licitante deverá possuir, em seu quadro de funcionários, técnicos especializados para os serviços solicitados, com certificação emitida pelo fabricante da solução.

12.2.5.16. Não será necessária a comprovação ponto a ponto dos itens presentes no Termo de Referência. A Comissão de Licitação poderá solicitar, na fase de análise das propostas, informações adicionais às proponentes, tais como folhetos, datasheets, manuais das soluções, produtos e serviços ofertados, além de realizar diligências para esclarecer e certificar-se de que todas as exigências técnicas mínimas estabelecidas no Termo de Referência estão sendo plenamente atendidas.

## 13. DAS OBRIGAÇÕES DAS PARTES

13.1. Será de responsabilidade da licitante vencedora, sob pena de aplicação das sanções previstas neste Edital e no Contrato:

a) Fornecer o objeto deste Edital de acordo com as especificações exigidas;

b) Fornecer o objeto desta licitação na forma, nos locais, nos prazos e nos preços estipulados em sua proposta;

c) Prestar garantia pelo período solicitado em cada item, conforme sua exigência;

d) Responsabilizar-se por todas as despesas e custos decorrentes das entregas, bem como por eventuais trocas durante o período de garantia;

e) Enviar por e-mail o arquivo XML resultante da emissão do DANFE para os endereços eletrônicos de cada Órgão Participante;

f) Manter as condições de habilitação e qualificação exigidas na licitação e comprovar a regularidade fiscal e trabalhista junto ao Órgão Gerenciador;

g) Acusar o recebimento das Autorizações de Fornecimento, bem como de quaisquer outras notificações enviadas por meio eletrônico, no prazo máximo de 24 (vinte e quatro) horas. Se o prazo final recair em final de semana ou feriado, será prorrogado para o próximo dia útil;

h) Emitir Nota Fiscal dos produtos e/ou serviços realizados, discriminando-os individual e pormenorizadamente, especificando quantitativos, marcas e modelos;

i) Destacar na nota fiscal emitida o valor de todos os tributos passíveis de retenção pelo Órgão Participante, nos termos da legislação em vigor, especialmente o IRRF, conforme a IN RFB 1.234/2012.

13.2. Será de responsabilidade do Órgão Participante:

a) Efetuar o pagamento dos produtos contratados nos prazos previstos;

b) Fiscalizar os fornecimentos, relatando problemas e circunstâncias que facilitem a prestação dos serviços;

c) Indicar prepostos para contato com os responsáveis da fornecedora;

d) Cumprir as obrigações previstas no Edital e nesta ata, exigindo o cumprimento das obrigações da contratada;

e) Atender às demais disposições contidas neste Edital, seus anexos, e na legislação aplicável.

## 13. DOS CRITÉRIOS DE JULGAMENTO E ADJUDICAÇÃO

13.1. A presente licitação será adjudicada à licitante que apresentar a proposta de MENOR PREÇO, em JULGAMENTO GLOBAL, desde que atendidas as demais exigências deste Edital.

## 14. DA IMPUGNAÇÃO DO EDITAL

15.1. Decairá do direito de impugnar os termos do Edital aquele que não o fizer **até 03 (três) dias úteis antes da data designada para a realização do Pregão**, devendo apontar de forma clara e objetiva as falhas e/ou irregularidades que entende viciarem o mesmo.

15.2. Serão admitidas as seguintes formas de impugnação do Edital:

a) Por intermédio de meio eletrônico, **exclusivamente** através da **PLATAFORMA ELETRÔNICA**: www.licitacimlago.com.br, no "Acesso Identificado", sendo aceita até às 23h59 da data limite estipulada.

b) **NÃO** será aceito pedido de esclarecimento ou impugnação por e-mail.

15.3. Caberá ao(à) Pregoeiro(a) decidir, **no prazo de 3 (três) dias úteis, limitado ao último dia útil anterior à data de abertura do certame**, sobre a impugnação interposta no que se refere aos procedimentos de licitação, podendo ser auxiliado pela equipe técnica no que tange a

avaliações dos produtos, normas e outros temas que não sejam de conhecimento técnico ou especializado do(a) Pregoeiro(a).

15.4. Se procedente e acolhida a impugnação do Edital, seus vícios serão sanados, reabrindo-se o prazo inicialmente estabelecido, exceto quando, inquestionavelmente, a alteração não comprometer a formulação das propostas.

## 15. DA ATA DE REGISTRO DE PREÇOS E DO CONTRATO DE FORNECIMENTO

16.1 As obrigações decorrentes das aquisições do objeto, constantes no Registro de Preços, a serem firmadas entre o Órgão Gerenciador (Consórcio Intermunicipal Multifinalitário dos Municípios do Lago de Furnas – CIMLAGO) e o fornecedor, com manifestação dos Órgãos Participantes, serão formalizadas através da Ata de Registro de Preços. O prazo de validade do Registro de Preços será de 12 (doze) meses, podendo ser prorrogado por igual período.

15.1.1. Em caso de prorrogação da vigência da Ata de Registro de Preços, as quantidades inicialmente registradas serão renovadas na sua totalidade, independentemente do quantitativo utilizado durante o período de vigência, não sendo permitido acumular as quantidades não utilizadas.

15.1.2. Os Órgãos Participantes, os fornecedores e os totais dos itens deste Edital estarão registrados na Ata de Registro de Preços Consolidada (ANEXO XII).

15.2. O fornecedor classificado em 1º (primeiro) lugar nos preços registrados e devidamente habilitado será convocado a firmar as Atas de Registro de Preços no prazo de 3 (três) dias úteis após a homologação, podendo o prazo ser prorrogado uma vez, por igual período, quando solicitado pelo fornecedor e desde que o motivo seja justificado e aceito pela Administração do Consórcio Público. O proponente deve manter-se nas mesmas condições de habilitação quanto à regularidade fiscal.

15.2.1. As demais ocorrências de convocação do fornecedor para firmar a Ata de Registro de Preços terão as mesmas condições estabelecidas no item 16.2, após notificação.

15.3. A Ata de Registro de Preços deverá ser assinada por meio de certificação digital.

15.4. O licitante que, convocado para assinar as Atas de Registro de Preços, deixar de fazê-lo no prazo fixado será excluído e poderá sofrer as penalidades impostas por lei, após regular Processo Administrativo.

15.5. Na hipótese de o fornecedor primeiro classificado ter seu registro cancelado, não assinar, não aceitar ou não retirar as Atas de Registro de Preços de Fornecimento no prazo e nas condições estabelecidas, poderão ser convocados os fornecedores do Cadastro de Reserva, na ordem de classificação, e estes poderão sofrer as penalidades impostas por lei, após regular Processo Administrativo.

15.6. Excetuados os fornecedores mais bem classificados durante a fase competitiva, todos os demais licitantes formarão o Cadastro de Reserva de Fornecedores.

15.6.1. Os fornecedores do Cadastro de Reserva serão incluídos na respectiva ata da sessão na forma de anexo, seguindo a ordem de classificação do certame, conforme a última proposta apresentada durante a fase competitiva.

15.7. Observados os critérios e condições estabelecidas neste Edital e o preço registrado, os Órgãos Participantes poderão adquirir de mais de um fornecedor registrado, conforme a ordem de classificação, desde que razões de interesse público justifiquem e que o primeiro classificado não possua capacidade de fornecimento compatível com o solicitado.

15.8. A existência de preços registrados não obriga o Órgão Gerenciador ou os Órgãos Participantes a firmar as contratações que deles possam advir, sendo facultada a realização de licitação específica para a aquisição pretendida, assegurando-se ao beneficiário do registro a preferência de fornecimento em igualdade de condições.

## 16. DO REAJUSTE DOS PREÇOS

16.1. Os preços registrados não serão reajustados durante a vigência da Ata de Registro de Preços, mesmo se ela for prorrogada, entretanto, nesta situação de prorrogação da ata, as

partes deverão concordar formalmente em prorrogar a Ata de Registro de Preços sem majorar os valores de preços registrados originalmente.

## 17. DOS RECURSOS, RESPONSABILIDADES E PENALIDADES ADMINISTRATIVAS

18.1. Dos atos da Administração praticados neste certame, cabem:

a) Recurso, no **prazo de 03 (três) dias úteis**, contado da data de intimação ou de lavratura da ata, em face de:

a.1) Julgamento das propostas;

a.2) Ato de habilitação ou inabilitação de licitante;

a.3) Anulação ou revogação da licitação;

a.4) Extinção do contrato, quando determinada por ato unilateral e escrito da Administração;

b) Pedido de reconsideração, no **prazo de 03 (três) dias úteis**, contado da data de intimação, relativamente a ato do qual não caiba recurso hierárquico.

18.1.1. Quanto ao recurso apresentado com base nos itens **a.1** e **a.2** da alínea "a" do item 18.1, serão observadas as seguintes disposições:

I. A intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão, e o prazo para apresentação das razões recursais, previsto na alínea "a" do item 18.1, será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação;

II. A apreciação dar-se-á em fase única.

18.1.2. O recurso de que trata a alínea "a" do item 18.1 será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual, se não reconsiderar o ato ou a decisão **no prazo de 03 (três) dias úteis**, encaminhará o recurso, com sua motivação, à autoridade

superior, que deverá proferir sua decisão no prazo máximo de 10 (dez) dias úteis, contados do recebimento dos autos.

18.1.3. O prazo para contrarrazões será o mesmo do recurso e terá início após encerrado o prazo das razões do recurso.

18.1.4. Será assegurado ao licitante o direito de vista dos elementos indispensáveis à defesa de seus interesses.

18.1.5. O recurso ou pedido de reconsideração deverá ser interposto da seguinte forma:

a) Por intermédio de meio eletrônico, exclusivamente através da PLATAFORMA ELETRÔNICA: www.licitacimlago.com.br, no "Acesso Identificado", sendo aceito até às 23h59 da data limite estipulada pelo(a) Pregoeiro(a);

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

18.2. Não sendo interpostos recursos, ou sendo interposto em desacordo com o Edital, ou decididos os recursos interpostos, o(a) Pregoeiro(a) encaminhará o processo licitatório para a Autoridade Competente para os procedimentos de adjudicação do objeto do certame à(s) empresa(s) declarada(s) vencedora(s) e homologação.

18.3. As causas de rescisão contratual estão estabelecidas no artigo 137, de acordo com as disposições dos artigos 138 e 139, todos da Lei Federal nº 14.133, de 2021.

18.3.1 Nas hipóteses de inexecução total ou parcial do contrato e das obrigações nele assumidas, o Órgão Gerenciador poderá aplicar ao fornecedor, em relação às contratações dos Órgãos Participantes, as seguintes sanções:

a) Advertência;

b) Impedimento de licitar e contratar com o Consórcio Intermunicipal Multifinalitário dos Municípios do Lago de Furnas – CIMLAGO, bem como com qualquer um dos municípios consorciados, por prazo não superior a **3 (três) anos**;

c) Em caso de atraso superior a **5 (cinco) dias** na entrega do objeto, o fornecedor será constituído em mora, sujeito a **multa de 0,5% (meio por cento)** por dia de atraso, incidente sobre o valor total do contrato, a ser calculada a partir do **6º (sexto)** dia de atraso até o efetivo cumprimento da obrigação, limitada a **30 (trinta) dias**;

d) Em caso de inexecução parcial ou de qualquer outra irregularidade no objeto, poderá ser aplicada multa de **10% (dez por cento)**, calculada sobre o valor do contrato, ou proporcionalmente por cada descumprimento;

e) Transcorridos **30 (trinta) dias** do prazo de entrega estabelecido no contrato, será considerado rescindido o contrato, cancelado o Registro de Preços, e aplicada uma **multa de 15% (quinze por cento)** por inexecução total, calculada sobre o valor da contratação. Dependendo do descumprimento, se gerar algum prejuízo ao CIMLAGO ou a qualquer um dos municípios consorciados, poderá ser requerido do fornecedor o valor correspondente a perdas e danos, conforme apuração em Processo Administrativo de reconhecimento da responsabilidade;

f) Declaração de inidoneidade, nos termos do art. 156, inciso IV e §§ 5º e 6º, da Lei Federal nº 14.133, de 2021.

17.4. O licitante ou contratado também será responsável administrativamente pelas infrações previstas no art. 155, da Lei Federal nº 14.133, de 2021.

17.5. A aplicação das sanções ao responsável pelas infrações administrativas seguirá as disposições previstas nos art. 156 a 163, da Lei Federal nº 14.133, de 2021.

17.6. Na hipótese de aplicação de penalidade de multa, após os procedimentos legais, será emitida notificação de cobrança ao licitante, que deverá fazer o recolhimento do valor no prazo estabelecido na decisão do processo administrativo, sob pena de cobrança judicial.

## 18. DAS ALTERAÇÕES DA ATA DE REGISTRO DE PREÇOS

18.1. A Ata de Registro de Preços poderá sofrer alterações, obedecidas às disposições contidas na Resolução 004/2024 ou outra que vier a substituir.

18.1.1. O preço registrado poderá ser revisto em decorrência de eventual redução daqueles praticados no mercado, ou de fato que eleve o custo dos serviços ou bens registrados, cabendo ao Órgão Gerenciador da Ata de Registro de Preços promover as necessárias negociações junto aos fornecedores.

18.1.2. Quando o preço inicialmente registrado, por motivo superveniente, tornar-se superior ao preço praticado no mercado o Órgão Gerenciador deverá:

I. Convocar o fornecedor visando a negociação para redução de preços e sua adequação ao praticado pelo mercado;

II. Frustrada a negociação, o fornecedor será liberado do compromisso assumido sem aplicação de penalidade; e

III. Convocar os demais fornecedores visando igual oportunidade de negociação.

18.1.3. Quando o preço de mercado se tornar superior aos preços registrados e o fornecedor, mediante requerimento devidamente comprovado, não puder cumprir o compromisso, o Órgão Gerenciador poderá:

I. Liberar o fornecedor do compromisso assumido, caso a comunicação ocorra antes do pedido de fornecimento, e sem aplicação da penalidade se confirmada a veracidade dos motivos e comprovantes apresentados; e

II. Convocar os demais fornecedores para assegurar igual oportunidade de negociação.

18.1.4. Não havendo êxito nas negociações, o Órgão Gerenciador deverá proceder à revogação da Ata de Registro de Preços, adotando as medidas cabíveis para obtenção da contratação mais vantajosa.

18.2. É possível realizar aumento nos quantitativos fixados pela Ata de Registro de Preços, até uma vez a quantidade registrada inicialmente, desde que com aceitação expressa do fornecedor, formalizada mediante apostilamento, quando caracterizadas circunstâncias supervenientes, devidamente demonstradas nos autos do procedimento administrativo em que tramitar a alteração, que indiquem que as estimativas inicialmente previstas neste edital serão insuficientes para atender a demanda durante o prazo de vigência.

## 19. DO CANCELAMENTO DO REGISTRO DE PREÇOS

20.1 O FORNECEDOR terá seu registro cancelado quando:

I. Descumprir as condições da Ata de Registro de Preços;

II. Não retirar a nota de empenho e ou autorização de fornecimento de compra no prazo estabelecido pela Administração, sem justificativa aceitável;

III. Não aceitar reduzir o seu preço registrado, na hipótese de este se tornar superior àqueles praticados no mercado;

IV. Tiver presentes razões de interesse público;

V. Sofrer sanções impeditivas previstas em lei;

VI. For declarado inidôneo ou impedido de licitar ou contratar com o Consórcio Intermunicipal Multifinalitário Dos Municípios Do Lago De Furnas – CIMLAGO ou com qualquer um dos Municípios Consorciados nos termos do artigo 156, inciso IV, da Lei Federal nº. 14.133, de 2021.

VII. Não utilizar recursos de tecnologia da informação disponibilizados pelo Consórcio Público na operacionalização e automatização dos procedimentos de controle da

execução do objeto contratual, quando for o caso.

19.1. O cancelamento do registro de preços, nas hipóteses previstas, assegurados o contraditório e a ampla defesa, será formalizado por despacho da autoridade competente do Órgão Gerenciador.

19.2. O cancelamento do registro de preços poderá ocorrer por fato superveniente, decorrente de caso fortuito ou força maior, que prejudique o cumprimento da ata, devidamente comprovados e justificados:

I. Por razão de interesse público; ou

II. A pedido do fornecedor.

## 20. DA DOTAÇÃO

20.1. As despesas decorrentes das aquisições, objeto do presente certame correrão a conta de dotação específica dos orçamentos de cada Órgão Participante, referente ao exercício de 2024.

## 21. DO CRITÉRIO DE MEDIÇÃO E DE PAGAMENTO

### 22.1. Recebimento:

22.1.1. 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.

22.1.2. 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 05 (cinco) dias uteis, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

22.1.3. 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.

22.1.4. 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.

22.5. 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 no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

22.1.6. 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.

22.1.7. 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.

22.2. Liquidação:

a) 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 desde que devidamente justificado.

b) 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:

i. O prazo de validade;

ii. A data da emissão;

iii. Os dados do contrato e do órgão CONTRATANTE;

iv. O período respectivo de execução do contrato;

v. O valor a pagar; e

vi. Eventual destaque do valor de retenções tributárias cabíveis.

c) 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;

d) A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta *on-line*, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.

e) Constatando-se, junto aos sítios eletrônicos à 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.

f) 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.

g) 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.

h) 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 aos órgãos de regularidade fiscais.

22.3. Prazo de Pagamento:

a) O pagamento será efetuado no prazo de 30 (trinta) dias contados da finalização da liquidação da despesa, conforme seção anterior.

b) Se o Órgão Participante não efetuar o pagamento no prazo previsto no Edital e na Ata de Registro de Preços, e tendo o Fornecedor, à época, adimplido integralmente as obrigações avençadas, inclusive quanto aos documentos que devem acompanhar a Nota Fiscal, os valores devidos serão monetariamente atualizados, a partir do dia de seu vencimento e até o dia de sua liquidação, segundo os mesmos critérios adotados para atualização de obrigações tributárias, conforme estabelecido no artigo 92, inciso V, da Lei Federal nº 14.133, de 2021.

22.4. Forma de Pagamento:

a) O pagamento pelas aquisições e/ou prestação de serviços, objeto da presente licitação, será feito pelo Órgão Participante em favor da licitante vencedora, mediante transferência bancária (TED, DOC, depósito ou PIX) em conta corrente de titularidade do Fornecedor ou boleto, após as entregas dos bens e/ou serviços, acompanhados da respectiva nota fiscal.

b) Poderão ser realizados pagamentos em contas cujo CNPJ de titularidade seja diverso daquele da habilitação e proposta vinculada no caso de solicitação de alteração entre o CNPJ da matriz e filiais ou de filiais entre si, mediante comprovação do preenchimento dos requisitos de habilitação pelo novo CNPJ.

c) As taxas bancárias (TED, DOC, PIX ou outras) não poderão ser descontadas do pagamento previsto neste item.

d) Na realização do pagamento serão retidos os Tributos devidos conforme as normas em vigor e passíveis de retenção pelo Órgão Participante, devendo o fornecedor indicar estes

valores no documento fiscal. Referente ao IRRF deverá ser observada a IN RFB 1.234/2012.

## 22. DA FISCALIZAÇÃO

23.1. A fiscalização da execução do objeto contratado será realizada pelo Gestor e Fiscal indicados pelo Município consorciado no momento do protocolo da intenção de registro de preço, de acordo com o Anexo I deste instrumento convocatório.

## 23. DAS DISPOSIÇÕES GERAIS

23.1. Caberá ao Órgão Gerenciador a prática de todos os atos de controle e administração do Sistema de Registro de Preços.

23.2. A existência de preços registrados não obriga o Órgão Gerenciador CIMLAGO ou os Órgãos Participantes a firmar as contratações que deles poderão advir, facultando-se a realização de licitação específica para a aquisição pretendida, desde que motivada, sendo assegurado ao beneficiário do registro a preferência de fornecimento em igualdade de condições.

23.3. A Empresa vencedora deverá declarar ao Órgão Gerenciador (ANEXO III), o domicílio eletrônico o qual será destinado ao gerenciamento da Ata de Registro de Preço e recebimento das autorizações de fornecimento, alerta de avisos, notificações e decisões administrativas.

23.4. Nenhuma indenização será devida às licitantes pela elaboração e/ou apresentação de documentação relativa ao presente Edital.

23.5. O resultado desta licitação estará à disposição dos interessados, na Central Executiva do CIMLAGO, logo após sua homologação e disponíveis na plataforma eletrônica do Portal Oficial de Licitações do CIMLAGO e no sítio eletrônico oficial: www.cimlago.org.br.

23.6. Detalhes não citados referentes ao fornecimento dos produtos, mas que a boa técnica leve a presumir a sua necessidade, não deverão ser omitidos, não sendo aceitas justificativas

para sua não apresentação.

23.7. O Autoridade Competente do CIMLAGO poderá revogar a licitação em face de razões de interesse público derivadas de fato superveniente devidamente comprovado, pertinente e suficiente para justificar tal conduta, devendo anulá-la por ilegalidade, de ofício ou por provocação de qualquer pessoa, mediante ato escrito e fundamentado, observadas as disposições da Lei Federal nº 14.133, de 2021.

23.8. O(a) Pregoeiro(a) e a Equipe de Apoio prestarão os esclarecimentos necessários, devendo ser enviados ao(a) Pregoeiro(a), até três dias anteriores à data fixada para abertura da sessão pública, exclusivamente por meio eletrônico via portal indicado neste Edital.

23.8.1. Após a abertura da sessão, eventuais dúvidas existentes e esclarecimentos necessários deverão ser manifestados através da plataforma www.licitacimlago.com.br.

23.8.1.1. Consultas a respeito de dúvidas ou esclarecimentos solicitadas fora dos parâmetros descritos no item 24.8.1 (como, por exemplo, através de “e-mail”), não serão respondidas.

23.8.1.2. As previsões dos itens 24.8, 24.8.1 e 24.8.1.1 dizem respeito às dúvidas e esclarecimentos, de maneira que eventuais inconformismos, discordâncias ou pedidos de reconsideração [dentre outros requerimentos] com relação a atos praticados nesta licitação deverão ser combatidos através de impugnação ou recurso, respeitando os procedimentos previstos neste edital.

23.9. Não cabe ao Portal Oficial de Licitações do CIMLAGO ou ao CIMLAGO qualquer responsabilidade pelas obrigações assumidas pelo fornecedor com o licitante, em especial com relação à forma e às condições de entrega dos bens ou da prestação de serviços e quanto à quitação financeira da negociação realizada.

23.10. O(a) Pregoeiro(a) e Equipe de Apoio foram nomeados através da Resolução n. 005/2024 do CIMLAGO.

23.11. São partes integrantes deste Edital os seguintes ANEXOS:

ANEXO I – Termo de Referência;

ANEXO II – Modelo de Proposta de Preços

ANEXO III – Dados bancários, dados do representante legal, declaração de domicílio eletrônico da Empresa e declaração de assinatura por certificação digital;

ANEXO IV – Declaração de Cumprimento Pleno aos Requisitos de Habilitação;

ANEXO V – Declaração de Ausência de Condenação

ANEXO VI – Declaração de Ausência de Vínculo;

ANEXO VII – Declaração de Microempresa ou Empresa de Pequeno Porte;

ANEXO VIII – Declaração de Enquadramento Receita Bruta;

ANEXO IX – Declaração de Cumprimento do artigo 7º, inciso XXXIII, da Constituição da República Federativa do Brasil;

ANEXO X – Declaração de Reservas de Cargos;

ANEXO XI – Minuta da Ata de Registro de Preços;

ANEXO XII – Minuta de Contrato Administrativo Licitatório.

Alfenas/MG, 26 de setembro de 2024.

Luiza Maria Lima Menezes
Presidenta CIMLAGO

ANEXO I – TERMO DE REFERÊNCIA

EDITAL DO PREGÃO, NA FORMA ELETRÔNICA, Nº 016/2024

PROCESSO ADMINISTRATIVO LICITATÓRIO ELETRÔNICO 016/2024

SISTEMA DE REGISTRO DE PREÇOS

## 1. DO OBJETO

1.1. O objeto deste processo licitatório é o REGISTRO DE PREÇOS, por meio de licitação compartilhada, para a eventual e futura aquisição de infraestrutura como serviço, abrangendo soluções de armazenamento inteligente, proteção e armazenamento de dados, soluções de redes, proteção de perímetro, *endpoint* e gerenciamento de vulnerabilidades, com a finalidade de proporcionar ampla capacidade de atendimento aos usuários dos sistemas, incluindo serviços de instalação, configuração, transferência de conhecimento técnico e gerenciamento do ambiente, destinados a suprir futuras demandas para atender os municípios consorciados ao Consórcio Intermunicipal Multifinalitário dos Municípios do Lago de Furnas – CIMLAGO.

## 2. DA JUSTIFICATIVA DA CONTRATAÇÃO

2.1. Com o avanço constante das tecnologias da informação e comunicação, surgem grandes oportunidades para modernizar a infraestrutura digital e aprimorar a **segurança e eficiência** no gerenciamento de dados públicos. A implementação de soluções inteligentes de armazenamento e proteção de dados, além de redes seguras, permite não apenas **reduzir custos operacionais** e aumentar a **proteção contra ameaças cibernéticas**, mas também **otimizar a prestação de serviços públicos**. Isso resulta em maior confiabilidade, continuidade dos serviços e um alinhamento mais eficaz com as necessidades de modernização dos municípios, promovendo **inovação e segurança** no gerenciamento de informações críticas.

2.2. Esse cenário não só proporciona maior **eficiência na administração pública**, mas também possibilita que a continuidade dos serviços essenciais seja mantida, mesmo em situações de

incidentes tecnológicos ou falhas operacionais. Ao garantir a **disponibilidade e integridade dos dados**, essas soluções permitem que as áreas responsáveis atuem de maneira mais ágil e assertiva, minimizando o impacto de interrupções e assegurando que as **informações críticas** estejam sempre acessíveis e seguras.

2.3. Além disso, a modernização da infraestrutura tecnológica também contribui para a **automação dos processos** e o fortalecimento da **gestão de vulnerabilidades**, que são cada vez mais necessários diante do aumento das ameaças cibernéticas. Com isso, será possível não apenas atender às **exigências legais e normativas** relacionadas à proteção de dados, mas também elevar o nível de confiança e transparência no uso dos recursos tecnológicos para benefício da sociedade.

2.4. Por fim, o investimento em **infraestrutura como serviço**, que inclui soluções de armazenamento inteligente, proteção de perímetro, gerenciamento de vulnerabilidades, e automação de processos, é um passo essencial para garantir a **modernização dos sistemas** e o **desenvolvimento sustentável** das organizações. Esse avanço tecnológico proporcionará **maior segurança, eficiência e continuidade**, consolidando um padrão elevado de gestão pública em um ambiente cada vez mais digital e interconectado.

## 3. DAS ESPECIFICAÇÕES TÉCNICAS DO OBJETO

### 3.1. SERVIÇO DE ARMAZENAMENTO INTELIGENTE

| Item | Especificação de Hardware | Quantidade | Quantidade Total de Núcleos por servidor | Volumetria de Memória RAM (GB) por servidor | Volumetria Total (Bruta) de Discos SSD (TB) por servidor |
|---|---|---|---|---|---|
| 1.1 | Servidor | 3 | 14 | 64 | 4 |

Tabela 1: Modelo de Especificação Técnica por Servidor

### 3.2. CARACTERÍSTICAS DO SERVIDOR

3.2.1. Deverá ser oferecido um cluster com, no mínimo, 3 (três) equipamentos, conforme descrito a seguir:

3.2.2. Os servidores deverão ter, no máximo, 1 (uma) unidade de rack de altura (1U).

3.2.3. O hardware deverá ser devidamente testado e homologado para a solução de armazenamento inteligente proposta.

3.2.4. Cada chassi deverá conter, no mínimo, 1 (uma) fonte de alimentação.

3.2.5. Cada servidor deverá atender às seguintes especificações:

3.2.5.1. Possuir 1 (um) processador físico padrão x86. Cada processador deverá ter capacidade mínima de 14 (catorze) núcleos físicos e 20 (vinte) threads, além de suportar conjunto de instruções de 64 bits. A especificação dos processadores deverá estar em conformidade com a Tabela 1;

3.2.5.2. Suportar até 64 GB de memória RAM DDR4, conforme a Tabela 1;

3.2.5.3. Possuir, no mínimo, 1 (um) disco de estado sólido (SSD) padrão M.2 NVMe, conforme volumetria especificada na Tabela 1;

3.2.5.4. Contar com, no mínimo, 2 (duas) portas 2.5 Gigabit Ethernet padrão RJ-45;

3.2.5.5. Possuir 1 (uma) porta VGA ou HDMI;

3.2.5.6. Contar com 2 (duas) portas USB 3.0 ou superior;

3.2.5.7. No painel frontal do chassi, deverá haver um botão de energia e luzes indicativas de alerta.

3.2.6. O equipamento deverá ser fornecido com todos os acessórios necessários para sua instalação, incluindo, mas não se limitando a trilhos para montagem em rack e cabos de alimentação.

## 3.3. DO LICENCIAMENTO DO SOFTWARE DA SOLUÇÃO DE ARMAZENAMENTO INTELIGENTE

3.3.1. O software de armazenamento inteligente destinado ao Servidor Tipo 1 deverá ser licenciado por site.

3.3.1.1. O licenciamento por site deverá permitir a execução de até 15 (quinze) máquinas virtuais.

3.3.1.2. O licenciamento por site deverá autorizar o uso de até 8 (oito) unidades do Servidor Tipo 1 em um mesmo cluster na mesma localidade. O licenciamento deverá ser fornecido para essa quantidade, independentemente do formato ou tipo de licenciamento comercializado pelo fabricante da solução.

## 3.4. DAS DESCRIÇÕES GERAIS DA SOLUÇÃO DE ARMAZENAMENTO INTELIGENTE

3.4.1. A solução de armazenamento inteligente deverá ser composta por todos os equipamentos e softwares descritos neste Termo de Referência, incluindo o licenciamento de software necessário para o pleno atendimento às especificações técnicas durante a prestação do serviço.

3.4.2. A solução proposta, tanto de hardware quanto de software, deverá existir como um produto único antes da publicação deste edital, caracterizando-se como uma tecnologia integrada de armazenamento e processamento.

3.4.3. Para os fins deste edital, a denominação "servidor" será sinônima de "nó", "*appliance*" ou "lâmina".

3.4.4. A solução deverá prover uma infraestrutura integrada de alta disponibilidade em configuração de cluster para ambientes virtualizados. Não serão aceitas soluções ou funcionalidades implementadas via software ainda em fase de desenvolvimento, ou seja, aquelas que ainda não foram homologadas para ambientes de produção.

3.4.5. A solução deverá possuir um virtualizador baseado em Linux KVM, que seja suportado e mantido pelo fabricante da solução de armazenamento inteligente, e que contenha todas as características descritas nos itens e subitens relativos às propriedades do hipervisor.

3.4.6. A solução deve permitir a hospedagem de serviços de Tecnologia da Informação, instalados em máquinas virtuais que operem com os sistemas Linux, CentOS Enterprise Linux, RHEL Enterprise Linux, Ubuntu Server, SUSE Linux Enterprise, e Microsoft Windows Server em suas versões mais recentes suportadas pelos respectivos fabricantes.

3.4.7. A solução deverá permitir a expansão do cluster por meio da adição de novos servidores ao ambiente.

3.4.8. A solução deverá suportar servidores com diferentes especificações de hardware, tanto no cluster atual quanto em futuras expansões, incluindo servidores com diferentes configurações de processadores, memória RAM, armazenamento híbrido ou *all-flash*.

3.4.9. A solução deverá ser compatível e estar homologada para os servidores descritos na Tabela 1.

## 3.5. DOS REQUISITOS DE GERENCIAMENTO DA SOLUÇÃO DE ARMAZENAMENTO INTELIGENTE

3.5.1. Toda a solução, incluindo hardware e software, deverá ser gerenciada por meio de uma única interface web, acessível a partir de qualquer servidor do cluster.

3.5.2. A interface deverá ser simples e permitir o gerenciamento de recursos de armazenamento, computação e máquinas virtuais, a partir de uma única interface.

3.5.3. A solução deverá apresentar estatísticas de recursos em tempo real, incluindo IOPS, tanto por máquina virtual quanto pelo cluster.

3.5.4. A interface web deverá exibir estatísticas de recursos por máquina virtual.

3.5.5. A solução deverá contar com uma console de administração web em alta disponibilidade.

3.5.6. A console web deverá ser acessível por navegadores que suportem a tecnologia HTML5.

3.5.7. A solução deverá permitir a criação de vários usuários, com credenciais de acesso exclusivas.

3.5.8. A console web deverá permitir integração com o *Active Directory* da Microsoft para autenticação ou, alternativamente, utilizar autenticação local.

3.5.9. Com o objetivo de automatizar os processos de implementação, manutenção e gerenciamento do cluster, o sistema operacional em execução na solução integrada deverá oferecer APIs REST.

3.5.10. A solução deverá possuir uma interface de linha de comando.

3.5.11. A console web centralizada deverá suportar o gerenciamento de múltiplos clusters ou nós únicos, dispersos geograficamente. Para os sistemas remotos, deverá ser possível monitorar erros e alertas, facilitando a rápida resolução de problemas.

3.5.12. A interface IPMI ou similar, presente em cada um dos servidores, deverá ser baseada em Web e acessível por meio de um endereço IP. No mínimo, as seguintes funcionalidades deverão estar disponíveis na interface web:

3.5.12.1. Console remoto gráfico;

3.5.12.2. Ligar, desligar e reiniciar o servidor remotamente;

3.5.12.3. Monitoramento do hardware;

3.5.12.4. Atualização do software IPMI ou similar através da console web.

3.5.12.4.1. Este item não se aplica aos servidores com um único disco.

3.5.13. A console de administração gráfica deverá disponibilizar, quando necessário, o acesso remoto ao time de suporte do fabricante. Essa funcionalidade deverá estabelecer um túnel

ou mecanismo similar para conectar aos servidores do fabricante, permitindo ao suporte executar manutenções no software de armazenamento inteligente. O administrador do sistema poderá habilitar ou desabilitar o acesso a qualquer momento.

3.5.14. A solução deverá ser capaz de fornecer alertas do sistema.

3.5.15. Os alertas deverão ser emitidos via console web, e-mail e SNMP.

## 3.6. DAS CARACTERÍSTICAS DA SOLUÇÃO DE ARMAZENAMENTO INTELIGENTE

3.6.1. Serão aceitas soluções de armazenamento inteligente baseadas exclusivamente no nível de kernel do virtualizador.

3.6.2. A solução deverá replicar automaticamente todas as gravações para um ou mais servidores do cluster, utilizando as interfaces de maior *throughput* presentes em cada servidor, as quais deverão ter, no mínimo, 10 Gbps, com redundância.

3.6.2.1. Para servidores com um único disco, as replicações das gravações poderão ser realizadas através de interface de 1 Gbps.

3.6.3. A solução deverá garantir que os dados estejam sempre gravados em mais de um servidor simultaneamente.

3.6.4. A solução deverá suportar a falha de 1 (um) servidor por cluster.

3.6.5. Deverá permitir escalabilidade horizontal, ou seja, a adição de novos chassis ou servidores ao cluster, por meio de uma console gráfica, sem a interrupção do ambiente de produção, aumentando a capacidade de armazenamento, processamento e memória disponibilizados ao hipervisor, além de garantir um crescimento linear no desempenho do cluster.

3.6.6. O processo de escrita dos dados na solução de armazenamento inteligente deverá utilizar todos os discos disponíveis, sejam eles SSDs ou HDDs.

3.6.6.1. Não serão aceitas soluções de armazenamento inteligente que necessitem de discos dedicados exclusivamente para cache.

3.6.7. A solução deverá possuir funcionalidade de tierização de dados entre camadas de discos SSD e HDD.

3.6.8. A solução deverá permitir que uma máquina virtual seja executada exclusivamente em discos flash (SSD) ou exclusivamente em discos rígidos (HDD), conforme necessário.

3.6.9. A falha de um disco SSD ou HDD não deverá impactar a disponibilidade de um servidor no cluster.

3.6.9.1. Este item não se aplica para servidores com um único disco.

3.6.10. A solução deverá operar com o conceito de pool de armazenamento, composto por todos os discos presentes no cluster. O pool de armazenamento deverá ser expansível com a adição de novos discos à medida que novos servidores forem incorporados ao cluster.

3.6.11. A solução deverá possibilitar a atualização dos servidores do cluster de forma simples e automatizada, sem a necessidade de intervenção manual do administrador e sem a interrupção completa do ambiente. As atualizações deverão abranger os seguintes componentes:

3.6.11.1. O sistema de armazenamento distribuído e definido por software, baseado em kernel;

3.6.11.2. O hipervisor.

3.6.12. A solução deverá prover desduplicação pós-processo, utilizando técnicas de processamento paralelo distribuído para otimizar a capacidade de armazenamento.

3.6.13. A solução deverá fornecer snapshots nativos por máquina virtual, armazenando-os no cluster para proteção local. Os snapshots criados deverão garantir a consistência de erros, ou

seja, poderão ser feitos com o ambiente em produção, assegurando a proteção dos dados gravados em disco e a integridade do sistema operacional da máquina virtual (VM).

3.6.14. A solução deverá fornecer snapshots nativos por máquina virtual, armazenando-os no cluster para proteção local, com consistência de aplicação, garantindo que todas as transações em andamento sejam pausadas momentaneamente para assegurar que as aplicações em execução não possuam snapshots com transações incompletas.

3.6.15. A solução deverá permitir a recuperação granular de arquivos com base nos snapshots.

3.6.16. A solução deverá possuir funcionalidade de replicação de software integrada.

3.6.17. A solução deverá suportar, nativamente e sem a necessidade de integração com produtos de terceiros, replicação com um RPO (*Recovery Point Objective*) mínimo de 5 minutos entre dois sites.

3.6.18. A replicação deverá ser realizada apenas dos blocos alterados para o site secundário.

3.6.18.1. A replicação deverá ser realizada para um cluster, utilizando a mesma tecnologia proposta, nas dependências da CONTRATANTE.

3.6.18.2. A funcionalidade de replicação nativa da solução deverá operar com snapshots das máquinas virtuais e suportar as seguintes topologias de interconexão entre clusters em diferentes localidades: um para um e vários para um.

## 3.7 DO RACK DE DATACENTER

3.7.1. Deverá ser fornecido um rack padrão para Datacenter com as seguintes especificações:

3.7.2. Deverá possuir 24 (vinte e quatro) unidades de rack disponíveis para a alocação de ativos de TI.

3.7.3. Deverá ter altura de até 1,20 metros.

3.7.4. Deverá ter largura de até 600 milímetros (60 cm).

3.7.5. Deverá ter profundidade máxima de até 1,10 metros.

3.7.6. O rack deverá cumprir as seguintes normas de segurança e qualidade:

3.7.6.1. RoHS (Restrição de Substâncias Perigosas);

3.7.6.2. Diretriz REACH (Registro, Avaliação, Autorização e Restrição de Substâncias Químicas);

3.7.6.3. PEP (Perfil Ambiental de Produto);

3.7.6.4. EOLI (End of Life Instructions).

3.7.7. O rack deverá possuir porta frontal com fechadura para garantir a segurança dos ativos de TI.

3.7.8. Deverá contar com portas traseiras divididas para facilitar o gerenciamento de cabos e conexões.

3.7.9. Deverá possuir divisórias de unidades de rack (Rack Units) para otimizar o gerenciamento do espaço.

3.7.10. O rack deverá ter garantia e suporte técnico durante o período contratual de 12 (doze) meses, com atendimento na modalidade 24x7x365, incluindo a troca de peças no próximo dia útil, em horário comercial.

## 3.8 DAS CARACTERÍSTICAS DO VIRTUALIZADOR DA SOLUÇÃO DE ARMAZENAMENTO INTELIGENTE

3.8.1. O hipervisor proposto deverá possuir, no mínimo, as seguintes características:

3.8.1.1. Integração total com a solução proposta.

3.8.1.2. Licenciamento necessário para o pleno atendimento às especificações técnicas deste edital, durante toda a vigência da garantia e suporte.

3.8.1.3. Não serão aceitos hipervisores que estejam em fase de desenvolvimento ou homologação.

3.8.1.4. Capacidade de criação de máquinas virtuais compatíveis com, no mínimo, os seguintes sistemas operacionais em suas versões atuais mantidas pelos respectivos fabricantes:

3.8.1.4.1. Microsoft Windows Server;

3.8.1.4.2. Microsoft Windows;

3.8.1.4.3. Red Hat Enterprise Linux;

3.8.1.4.4. Linux CentOS;

3.8.1.4.5. Linux Ubuntu Server;

3.8.1.4.6. FreeBSD;

3.8.1.4.7. SUSE Linux Enterprise Server.

3.8.2. Permitir a criação de novas máquinas virtuais através de interface gráfica.

3.8.3. Possibilitar alterações de configurações (CPU, memória, disco e rede) em máquinas virtuais existentes por meio de interface gráfica.

3.8.4. Possuir interface gráfica para o gerenciamento de recursos como CPU, memória e I/O das máquinas virtuais.

3.8.5. Permitir que as máquinas virtuais utilizem diferentes redes virtuais em um mesmo servidor.

3.8.6. Permitir a criação de ambientes de alta disponibilidade a partir do hipervisor, com a formação de clusters entre os servidores físicos, garantindo que, em caso de indisponibilidade de um servidor, as máquinas virtuais sejam redistribuídas automaticamente entre os demais servidores, sem necessidade de intervenção manual.

3.8.7. Permitir a movimentação online de máquinas virtuais entre diferentes servidores.

3.8.8. Possuir recurso de virtualização para uma ou mais placas de rede.

3.8.9. Possibilitar a criação de novas máquinas virtuais a partir de modelos predefinidos, prontos para serem instalados em qualquer cluster sobre o virtualizador de qualquer servidor físico que componha a solução integrada.

3.8.10. Monitorar a utilização individual de cada máquina virtual criada.

3.8.11. Possibilitar a execução de comandos de parar, iniciar, suspender e resetar máquinas virtuais.

3.8.12. Permitir a disponibilização de placas de aceleração gráfica de forma virtualizada.

## 3.9. EXPANSÃO DE SERVIÇO DE ARMAZENAMENTO INTELIGENTE

| Item | Especificação de Hardware | Quantidade | Quantidade Total de Núcleos por servidor | Volumetria de Memória RAM (GB) por servidor | Volumetria Total (Bruta) de Discos SSD (TB) por servidor |
|---|---|---|---|---|---|
| 1.1 | Servidor | 1 | 14 | 64 | 4 |

Tabela 2: Modelos de especificação por servidor.

## 3.10 CARACTERÍSTICAS DO SERVIDOR

3.10.1. Deverá ser oferecido um servidor conforme as especificações abaixo:

3.10.2. O servidor deverá ter, no máximo, 1 (uma) unidade de rack de altura (1U).

3.10.3. O hardware deverá ser testado e homologado para a solução de armazenamento inteligente proposta.

3.10.4. Cada chassi deverá possuir, no mínimo, 1 (uma) fonte de alimentação.

3.10.5. Cada servidor deverá atender às seguintes especificações:

3.10.5.1. Possuir 1 (um) processador físico padrão x86, com capacidade mínima de 14 (catorze) núcleos físicos e 20 (vinte) threads, além de suporte para conjunto de instruções de 64 bits. Especificações dos processadores conforme Tabela 1;

3.10.5.2. Suportar até 64 GB de memória RAM DDR4, conforme a Tabela 1;

3.10.5.3. Possuir, no mínimo, 1 (um) disco de estado sólido (SSD) padrão M.2 NVMe, conforme volumetria especificada na Tabela 1;

3.10.5.4. Possuir, no mínimo, 2 (duas) portas Ethernet 2.5 Gigabit padrão RJ-45;

3.10.5.5. Possuir 1 (uma) porta VGA ou HDMI;

3.10.5.6. Possuir 2 (duas) portas USB 3.0 ou superior;

3.10.5.7. O painel frontal do chassi deverá conter um botão de energia e luzes indicativas de alertas.

3.10.6. O equipamento deverá ser fornecido com todos os acessórios necessários para sua instalação, incluindo, mas não se limitando a trilhos para montagem em rack e cabos de alimentação.

## 3.11 DO LICENCIAMENTO DO SOFTWARE DA SOLUÇÃO DE ARMAZENAMENTO INTELIGENTE

3.11.1. O software de armazenamento inteligente destinado ao Servidor Tipo 1 deverá ser licenciado por site.

3.11.1.1. O licenciamento por site deverá permitir a execução de até 15 (quinze) máquinas virtuais.

3.11.1.2. O licenciamento por site deverá permitir o uso de até 8 (oito) unidades do Servidor Tipo 1 em um mesmo cluster na mesma localidade. O licenciamento deverá ser fornecido para essa quantidade, independentemente do formato ou tipo de licenciamento comercializado pelo fabricante da solução.

## 3.12 DAS DESCRIÇÕES GERAIS DA SOLUÇÃO DE ARMAZENAMENTO INTELIGENTE

3.12.1. A solução de armazenamento inteligente deverá ser composta por todos os equipamentos e softwares especificados neste Termo de Referência, incluindo o licenciamento de software necessário para o pleno atendimento às especificações técnicas durante a prestação do serviço.

3.12.2. A solução proposta, incluindo hardware e software, deverá existir como um produto único antes da publicação deste edital, caracterizando-se como uma tecnologia integrada de armazenamento e processamento.

3.12.3. Para os fins deste edital, a denominação "servidor" será sinônima de "nó", "*appliance*" ou "lâmina".

3.12.4. A solução deverá prover uma infraestrutura integrada de alta disponibilidade em configuração de cluster para ambientes virtualizados. Não serão aceitas soluções ou funcionalidades implementadas via software que ainda estejam em fase de desenvolvimento, ou seja, que não tenham sido homologadas para ambientes de produção.

3.12.5. A solução deverá incluir um virtualizador baseado em Linux KVM, suportado e mantido pelo fabricante da solução de armazenamento inteligente, e que possua todas as características descritas nos itens e subitens que compõem as propriedades do hipervisor.

3.12.6. A solução deverá permitir a hospedagem de serviços de Tecnologia da Informação instalados em máquinas virtuais que operem com os sistemas Linux, CentOS Enterprise Linux,

RHEL Enterprise Linux, Ubuntu Server, SUSE Linux Enterprise, e Microsoft Windows Server, em suas versões mais recentes suportadas pelos respectivos fabricantes.

3.12.7. A solução deverá permitir a expansão do cluster por meio da adição de novos servidores ao ambiente.

3.12.8. A solução deverá suportar servidores com diferentes especificações de hardware, tanto no cluster atual quanto em futuras expansões, incluindo servidores com diferentes configurações de processadores, memória RAM, e armazenamento híbrido ou *all-flash*.

3.12.9. A solução deverá ser compatível e estar homologada para os servidores especificados na Tabela 2.

## 3.13 DOS REQUISITOS DE GERENCIAMENTO DA SOLUÇÃO DE ARMAZENAMENTO INTELIGENTE

3.13.1. Toda a solução, incluindo hardware e software, deverá ser gerenciada a partir de uma única interface web, acessível a partir de qualquer servidor no cluster.

3.13.2. A interface deverá ser simples e permitir o gerenciamento de recursos de armazenamento, computação e máquinas virtuais a partir de uma única interface.

3.13.3. A solução deverá apresentar estatísticas de recursos em tempo real, incluindo IOPS, tanto por máquina virtual (VM) quanto pelo cluster.

3.13.4. A interface web deverá exibir estatísticas de recursos por máquina virtual.

3.13.5. A solução deverá possuir uma console de administração web em alta disponibilidade.

3.13.6. A console web deverá ser acessível por navegadores que suportem a tecnologia HTML5.

3.13.7. A solução deverá permitir a criação de vários usuários, com credenciais de acesso exclusivas.

3.13.8. A console web deverá permitir integração com o Active Directory da Microsoft para autenticação, ou, alternativamente, utilizar autenticação local.

3.13.9. Para automatizar os processos de implementação, manutenção e gerenciamento do cluster, o sistema operacional da solução integrada deverá oferecer APIs REST.

3.13.10. A solução deverá possuir uma interface de linha de comando.

3.13.11. A console web centralizada deverá suportar o gerenciamento de múltiplos clusters ou nós únicos dispersos geograficamente. Para sistemas remotos, deverá ser possível monitorar erros e gerar alertas para rápida resolução de problemas.

3.13.12. A interface IPMI, ou similar, presente em cada um dos servidores deverá ser baseada na web, acessível através de um endereço IP. No mínimo, as seguintes opções deverão estar disponíveis na interface web:

3.13.12.1. Console remoto gráfico;

3.13.12.2. Ligar, desligar e reiniciar o servidor remotamente;

3.13.12.3. Monitoramento de hardware;

3.13.12.4. Atualização do software IPMI, ou similar, através da console web.

3.13.12.4.1. Este item não se aplica para servidores com um único disco.

3.13.13. A console de administração gráfica deverá disponibilizar, quando necessário, o acesso remoto ao time de suporte do fabricante. Essa funcionalidade deverá estabelecer um túnel ou mecanismo similar para permitir que o suporte execute manutenções no software de armazenamento inteligente. O administrador do sistema poderá habilitar ou desabilitar o acesso a qualquer momento.

3.13.14. A solução deverá ser capaz de fornecer alertas do sistema.

3.13.15. Os alertas deverão ser emitidos via console web, e-mail e SNMP.

## 3.14 DAS CARACTERÍSTICAS DA SOLUÇÃO DE ARMAZENAMENTO INTELIGENTE

3.14.1. Serão aceitas apenas soluções de armazenamento inteligente baseadas no nível de kernel do virtualizador.

3.14.2. A solução deverá replicar automaticamente todas as gravações para um ou mais servidores do cluster, utilizando as interfaces de maior throughput disponíveis em cada servidor, as quais deverão ter, no mínimo, 10 Gbps, com redundância.

3.14.2.1. Para servidores com um único disco, as replicações das gravações poderão ser realizadas através de uma interface de 1 Gbps.

3.14.3. A solução deverá garantir que os dados sejam sempre gravados em mais de um servidor simultaneamente.

3.14.4. A solução deverá suportar a falha de 1 (um) servidor por cluster.

3.14.5. A solução deverá permitir escalabilidade horizontal, ou seja, a adição de novos chassis ou servidores ao cluster por meio de uma console gráfica, sem necessidade de parar o ambiente de produção. Esse processo deverá aumentar a capacidade de armazenamento, processamento e memória do hipervisor, além de garantir o crescimento linear do desempenho do cluster.

3.14.6. O processo de escrita dos dados na solução de armazenamento inteligente deverá utilizar todos os discos disponíveis, sejam eles SSDs ou HDDs.

3.14.6.1. Não serão aceitas soluções de armazenamento inteligente que exijam discos dedicados exclusivamente para cache.

3.14.7. A solução deverá possuir funcionalidade de tierização de dados entre camadas de discos SSD e HDD.

3.14.8. A solução deverá implementar funcionalidade que permita que uma máquina virtual seja executada exclusivamente em discos flash (SSD) ou exclusivamente em discos rígidos (HDD).

3.14.9. A falha de um disco SSD ou HDD não deverá impactar a disponibilidade de um servidor no cluster.

3.14.9.1. Este item não se aplica para servidores com um único disco.

3.14.10. A solução deverá trabalhar com o conceito de pool de armazenamento, formado pelo conjunto de todos os discos presentes no cluster. O pool de armazenamento deverá ser expansível com a adição de novos discos à medida que novos servidores forem integrados ao cluster.

3.14.11. A solução deverá fornecer atualizações do tipo “menor esforço” em cada servidor, permitindo que todos os servidores do cluster sejam atualizados de forma simples e automatizada, eliminando a necessidade de intervenção manual do administrador e sem exigir a interrupção total do ambiente. Essa funcionalidade deverá atualizar os seguintes componentes:

3.14.11.1. O sistema de armazenamento distribuído e definido por software, baseado em kernel;

3.14.11.2. O hipervisor.

3.14.12. A solução deverá fornecer desduplicação pós-processo. A desduplicação deverá ocorrer após a gravação e utilizar técnicas de processamento paralelo distribuído para otimizar a capacidade de armazenamento.

3.14.13. A solução deverá prover snapshots nativos por máquina virtual, armazenando esses snapshots no cluster para proteção local. O snapshot criado deverá garantir a consistência de erros, podendo ser realizado com o ambiente em produção, assegurando a proteção dos dados gravados em disco e a integridade do sistema operacional da máquina virtual (VM).

3.14.14. A solução deverá prover snapshots nativos por máquina virtual, armazenando-os no cluster para proteção local. O snapshot deverá garantir a consistência da aplicação, pausando momentaneamente todas as transações em andamento para assegurar que as aplicações em execução não tenham snapshots com transações incompletas.

3.14.15. A solução deverá permitir a recuperação granular de arquivos com base nos snapshots.

3.14.16. A solução deverá possuir funcionalidade de replicação de software integrado.

3.14.17. A solução deverá suportar, nativamente e sem integração com produtos de terceiros, replicação com um RPO (Recovery Point Objective) mínimo de 5 minutos entre dois sites.

3.14.18. A solução deverá permitir a replicação apenas dos blocos alterados para o site secundário.

3.14.18.1. A replicação deverá ser realizada para um cluster, utilizando a mesma tecnologia proposta, nas dependências da CONTRATANTE.

3.14.18.2. A funcionalidade de replicação nativa da solução deverá trabalhar com snapshots das máquinas virtuais e suportar as seguintes topologias de interconexão entre clusters em diferentes localidades: um para um e vários para um.

## 3.15 DAS CARACTERÍSTICAS DO VIRTUALIZADOR DA SOLUÇÃO DE ARMAZENAMENTO INTELIGENTE

3.15.1. O hipervisor proposto deverá possuir, no mínimo, as seguintes características:

3.15.1.1. Integração total com a solução proposta.

3.15.1.2. Licenciamento necessário para o pleno atendimento às especificações técnicas deste edital, durante toda a vigência da garantia e suporte.

3.15.1.3. Não serão aceitos hipervisores que estejam em fase de desenvolvimento ou homologação.

3.15.1.4. Capacidade de criação de máquinas virtuais compatíveis com, no mínimo, os seguintes sistemas operacionais, em suas versões correntes mantidas pelos respectivos fabricantes:

3.15.1.4.1. Microsoft Windows Server;

3.15.1.4.2. Microsoft Windows;

3.15.1.4.3. Red Hat Enterprise Linux;

3.15.1.4.4. Linux CentOS;

3.15.1.4.5. Linux Ubuntu Server;

3.15.1.4.6. FreeBSD;

3.15.1.4.7. SUSE Linux Enterprise Server.

3.15.2. Permitir a criação de novas máquinas virtuais por meio de uma interface gráfica.

3.15.3. Possibilitar a alteração de configurações (CPU, memória, disco e rede) em máquinas virtuais existentes através de interface gráfica.

3.15.4. Possuir interface gráfica para o gerenciamento de recursos, como CPU, memória e I/O, das máquinas virtuais.

3.15.5. Permitir que as máquinas virtuais utilizem diferentes redes virtuais em um mesmo servidor.

3.15.6. Permitir a criação de ambientes de alta disponibilidade, com a formação de clusters entre os servidores físicos, garantindo que, em caso de indisponibilidade de um servidor, as

máquinas virtuais sejam redistribuídas automaticamente entre os demais servidores, sem necessidade de intervenção manual.

3.15.7. Permitir a movimentação online de máquinas virtuais entre diferentes servidores.

3.15.8. Possuir recurso de virtualização para uma ou mais placas de rede.

3.15.9. Possibilitar a criação de novas máquinas virtuais a partir de modelos predefinidos, prontos para serem instalados em qualquer cluster sobre o virtualizador de qualquer servidor físico que componha a solução integrada.

3.15.10. Monitorar a utilização individual de cada máquina virtual criada.

3.15.11. Possibilitar a execução de comandos para parar, iniciar, suspender e resetar máquinas virtuais.

3.15.12. Permitir a disponibilização de placas de aceleração gráfica de forma virtualizada.

## 3.16. SERVIÇO DE PROTEÇÃO DE DADOS

## 3.17. LICENCIAMENTO DA SOLUÇÃO DE PROTEÇÃO DE DADOS

**3.17.1.** O serviço de proteção de dados deverá estar licenciado para a proteção e restauração de 10 (dez) máquinas virtuais, mediante licenciamento perpétuo.

## 3.18 ARQUITETURA DA SOLUÇÃO DE PROTEÇÃO DE DADOS

3.18.1. A solução deve possuir um banco de dados ou catálogo interno contendo informações detalhadas sobre todos os arquivos e mídias nos quais os backups foram armazenados.

3.18.2. Devem ser incluídas todas as licenças de software de banco de dados necessárias para o armazenamento das informações, considerando a capacidade máxima do sistema.

3.18.3. A arquitetura da solução deve ser flexível e escalável, permitindo sua instalação, configuração e utilização em sites remotos interligados ao site principal por meio de WAN.

3.18.4. A solução deve prover recursos de desduplicação na origem e/ou no destino, além de compactação, tanto no site principal quanto nos sites remotos, dentro da capacidade previamente licenciada, sem necessidade de aquisição de qualquer outra licença ou recurso adicional para a execução dessas operações.

3.18.5. A solução de backup deve dispor de funcionalidade para otimizar o backup de sites remotos, assegurando que a transmissão de dados pela WAN seja minimizada, provendo tanto desduplicação quanto replicação, e possibilitando a recuperação granular de dados, permitindo tanto a recuperação total quanto parcial.

3.18.6. A solução de backup deve permitir o controle da largura de banda utilizada durante a operação de backup.

3.18.7. A solução de backup deverá estar licenciada para ser utilizada como destino direto (se necessário) de backup em fita, disco local em servidor, NAS, *appliance* e nuvem, devendo suportar armazenamento de objetos em Azure, AWS, GCP e OCI.

## 3.19 AMBIENTE VIRTUAL

3.19.1. O licenciamento para o ambiente virtual deverá ser baseado na quantidade de máquinas virtuais (VMs) protegidas.

3.19.2. Para esse ambiente, caso necessário, deverá permitir a instalação de agentes para backup online, sem a necessidade de aquisição de novas licenças.

3.19.3. Não deverá haver limite no *back-end* para armazenamento de backups, devendo permitir retenções e réplicas em quantidades ilimitadas.

## 3.20 FUNCIONALIDADES GERAIS DE BACKUP E RESTORE

3.20.1. A solução de backup deverá ser capaz de realizar backup de arquivos abertos sem comprometer sua consistência.

3.20.2. A solução de backup deverá possuir a funcionalidade de priorização de jobs de backup.

3.20.3. A solução de backup deverá possibilitar a paralelização da gravação de dados em dispositivos de armazenamento, por meio da funcionalidade conhecida como multiplexação.

3.20.4. A solução de backup deverá ser capaz de enviar alertas por e-mail, reportando eventos ocorridos durante a operação e configuração da solução.

3.20.5. A solução de backup deverá enviar *traps* SNMP (*Simple Network Management Protocol*) para reportar eventos ocorridos na operação da solução.

3.20.6. A solução de backup deverá possuir a funcionalidade de agendamento de *jobs* de backup.

3.20.7. Para operações de backup gravadas em disco e/ou fita, a solução de backup deverá possuir as seguintes funcionalidades:

3.20.8. Para um mesmo dado armazenado, deverá ser possível configurar diferentes períodos de retenção.

3.20.9. Para um dado armazenado, deverá ser possível estender o período de retenção.

3.20.10. A solução de backup deverá ser capaz de executar backups completos sintéticos. Um backup completo sintético é gerado com base em um backup completo tradicional (não sintetizado) anterior, juntamente com backups diferenciais subsequentes ou um backup incremental cumulativo. Esse backup sintetizado deverá permitir a restauração de arquivos e diretórios da mesma forma que um backup tradicional.

3.20.11. A solução deverá permitir a gravação de backups em diferentes topologias, como disco-para-disco-para-fita, disco-para-fita ou diretamente para fita, sendo sempre controlada pela ferramenta de backup.

3.20.12. A solução deverá ser compatível com bibliotecas autocarregadoras de cartuchos de fitas magnéticas.

3.20.13. A solução de backup deverá possuir a funcionalidade de criar múltiplas cópias de backups armazenados.

3.20.14. A solução deverá permitir a criação de perfis de acesso, possibilitando que grupos de pessoas tenham permissões específicas, como a recuperação de dados apenas na origem ou em outro local.

3.20.15. A solução de backup deverá implementar criptografia de dados tanto na origem (cliente de backup) quanto no destino, garantindo que os dados trafegados na rede local ou na WAN sejam criptografados, com suporte para chaves de, no mínimo, 128 bits.

3.20.16. Deverá possuir controle de acesso baseado em função (RBAC), permitindo que os usuários executem ações específicas conforme suas permissões.

3.20.17. A solução deverá ser capaz de integrar-se ao *Active Directory*, para a criação de usuários e atribuição de permissões administrativas.

3.20.18. Deverá ser possível criar usuários, atribuir funções, excluir funções e definir políticas de permissionamento de usuários.

## 3.21 FUNCIONALIDADES DA CONSOLE DE GERENCIAMENTO, INTEGRAÇÃO E ALTA DISPONIBILIDADE

3.21.1. A solução de backup deverá ser capaz de gerenciar e executar operações de *backup/restore* para os seguintes sistemas operacionais e ambientes: Windows, Linux e Unix (AIX, HP-UX); ambientes de virtualização VMware, Openstack, OVM, Hyper-V, Azure, AWS, GCP e OCI; aplicações como Microsoft Exchange Server, Microsoft SharePoint Server, Microsoft Active Directory e banco de dados Microsoft SQL Server, SAP, Oracle (Windows e Linux) e Oracle RAC (em Linux). Não serão aceitos backups baseados em scripts para esses ambientes.

3.21.2. O acesso administrativo ao console do servidor de gerenciamento de backup deverá ser realizado por meio de uma ferramenta gráfica disponibilizada pelo próprio software ou através de navegador Web.

3.21.3. A solução de backup deverá permitir a implementação de alta disponibilidade nos servidores. Em caso de falha de um dispositivo/equipamento, a solução não deverá ser impactada tanto no backup quanto no *restore*. Essa funcionalidade deverá estar totalmente integrada à solução de armazenamento.

3.21.4. A solução de backup deverá suportar Single Sign-On (SSO), permitindo integração com o Microsoft Active Directory e/ou LDAP.

3.21.5. A solução deverá oferecer suporte a autenticação de dois fatores (2FA).

3.21.6. A solução deverá suportar duplo fator de autorização, onde qualquer atividade de exclusão, seja de fitas, discos ou clientes, deverá ser autorizada por uma segunda pessoa.

3.21.7. O banco de dados para armazenamento do catálogo deverá possuir mecanismos de proteção (backup) e funcionalidades de recuperação rápida em caso de desastre.

3.21.8. A solução deverá prover deduplicação via software, tanto na origem quanto no destino, para 100% do licenciamento.

## 3.22 INTEGRAÇÃO COM AS SEGUINTES APLICAÇÕES PARA BACKUP E RESTORE

3.22.1. A solução deverá permitir a utilização de agentes online para backup de uma única pasta de um servidor de arquivos (Windows e Linux), NAS através do protocolo NDMP, e uma instância de banco de dados SQL, independentemente de o servidor ser físico ou virtual.

3.22.2. A solução de backup deverá realizar backup e *restore* para os seguintes sistemas operacionais e aplicativos, tanto em ambientes físicos quanto virtuais, utilizando agentes próprios ou ambientes de virtualização sem agentes, para pelo menos uma das últimas três versões dos sistemas operacionais e aplicações abaixo:

3.22.2.1. Microsoft Windows Server.

3.22.2.2. Oracle Linux.

3.22.2.3. Ubuntu Linux.

3.22.2.4. Red Hat Enterprise Linux.

3.22.2.5. AIX.

3.22.2.6. HP-UX.

3.22.2.7. Microsoft SQL Server.

3.22.2.8. Microsoft Exchange Server.

3.22.2.9. Microsoft SharePoint Server.

3.22.2.10. Oracle e Oracle RAC.

3.22.2.11. VMware vCenter.

3.22.2.12. Microsoft Hyper-V.

3.22.2.13. Oracle VM (OVM).

3.22.2.14. Openstack.

3.22.2.15. Kubernetes, Amazon EKS, Google Anthos, GKE, AKS, OKE e RHOCP.

3.22.2.16. Servidores virtuais em nuvens Microsoft Azure, Amazon EC2, GCP e OCI.

## 3.23. SUPORTE AO ACTIVE DIRECTORY

3.23.1. A solução deverá executar backup online do Microsoft Active Directory.

3.23.2. Deverá possibilitar as seguintes opções de recuperação:

3.23.3. Recuperação de um objeto.

## 3.24. SUPORTE AO MICROSOFT EXCHANGE SERVER:

3.24.1. A solução deverá executar backup e restore do Microsoft Exchange com as seguintes características:

3.24.2. Backup e restore das bases de dados do Exchange.

3.24.3. Backup e restore granular de mensagens, itens de calendário ou mailboxes.

3.24.4. Backup e restore de ambientes Exchange clusterizados (Fully Clustered DAG), tanto para servidores ativos quanto passivos.

3.24.5. Implementação de tecnologias de desduplicação de dados em ambientes Exchange.

## 3.25. SUPORTE A ORACLE E ORACLE RAC

3.25.1. A solução deverá executar backup e restore do Oracle e Oracle RAC, sem a necessidade de scripts, com as seguintes características:

3.25.2. Backup e restore das bases de dados Oracle/Oracle RAC via RMAN, sem interrupção do banco.

3.25.3. Backup de Archive Logs, permitindo a criação de rotinas de backup com intervalos definidos.

3.25.4. Configuração para que, após o backup dos Archive Logs, os mesmos sejam mantidos ou excluídos, conforme necessário.

## 3.26. A solução deverá possibilitar a recuperação com as seguintes características:

3.26.1. Recuperação completa da base de dados no mesmo servidor.

3.26.2. Recuperação completa da base de dados em outro servidor.

3.26.3. Recuperação de um *datafile* específico.

3.26.4. Recuperação granular no nível de tabela e/ou *tablespace*.

## 3.27. SUPORTE A MICROSOFT SQL SERVER

3.27.1. A solução deverá executar backup e *restore* do Microsoft SQL Server com as seguintes características nativas, sem a necessidade de criação de scripts;

3.27.2. Executar backup e *restore* das bases de dados do Microsoft SQL Server sem interrupção do banco;

3.27.3. A solução deverá possibilitar a recuperação com as seguintes características:

3.27.4. Recuperação completa da base de dados no mesmo servidor.

3.27.5. Recuperação completa da base de dados em outro servidor.

3.27.6. Recuperação de uma base de dados específica.

## 3.28. SUPORTE A SAP E SAP HANA

3.28.1. A solução deverá suportar BR Tools e BACKINT para backup e recuperação de bancos de dados SAP.

3.28.2. Deverá oferecer suporte à deduplicação de dados na origem (no servidor).

3.28.3. Deverá suportar restauração no próprio servidor (no sistema de origem) e também em outro servidor (em diferentes sistemas SAP de destino).

3.28.4. Deverá suportar backups completos e incrementais.

3.28.5. Deverá ser capaz de integrar-se ao HANA ou SAP HANA

## 3.29. SUPORTE AO AMBIENTE VIRTUAL (VMWARE E HYPER-V)

3.29.1. Deverá executar backup e restore do Ambiente Virtual com as seguintes características:

3.29.2. Realizar restore da imagem completa da máquina virtual (ambientes VMware, Hyper-V, OVM e Openstack) e de arquivos de maneira granular sem a necessidade de scripts.

3.29.3. No caso da restauração granular, não há necessidade de se restaurar a Guest VM inteira.

3.29.4. Permitir redirecionar a restauração de uma Guest VM para uma pasta alternativa, outro datastore, host ou rede.

3.29.5. Incluir automaticamente máquinas virtuais novas criadas dentro de seleções de backup anteriores.

3.29.6. Permitir o backup Full, Incremental e Sintético para os servidores virtuais.

3.29.7. Deverá ser capaz de realizar backups/restore de servidores virtuais Linux e Windows.

3.29.8. Deverá permitir que as tarefas de backup/recovery sejam realizadas via interface gráfica, sem a necessidade de scripts.

3.29.9. O backup dos servidores virtuais deverá ser armazenado de maneira desduplicada.

3.29.10. A solução de backup dos servidores virtuais deverá estar integrada à solução de Snapshot de hardware ou do hypervisor.

3.29.11. Para VMware, permitir iniciar uma máquina virtual diretamente do repositório de backup sem a necessidade de recuperá-la.

3.29.12. Deverá ser capaz de configurar um DR (Disaster Recovery) para VMs na Amazon.

3.29.13. Deverá ser capaz de fazer uma recuperação bare metal de máquinas físicas em VMs Hyper-V/VMs VMware a partir de dados de backup.

## 3.30. SUPORTE A PLATAFORMA DE NUVEM

3.30.1. Deve oferecer suporte ao backup de servidores virtuais na Amazon, Azure, Google Cloud e Oracle Cloud;

3.30.2. Deve ter a capacidade de fazer DR na nuvem (para cargas de trabalho locais) usando as cópias de backup armazenadas na nuvem

3.30.3. Deve ter a capacidade de oferecer suporte aos seguintes serviços de banco de dados em nuvem:

3.30.4. Mysql

3.30.5. Oracle

3.30.6. PostgreSQL

3.30.7. SQL

3.30.8. DocumentDB

3.30.9. DynamoDB

3.30.10. Cosmo DB

3.30.11. Redshift

3.30.12 MariaDB

3.30.13. Aurora

## 3.31. FUNCIONALIDADE DE DESDUPLICAÇÃO DA SOLUÇÃO DE PROTEÇÃO DE DADOS

3.31.1. A solução de backup deverá permitir o uso da tecnologia de desduplicação de dados para toda a capacidade licenciada, eliminando blocos repetidos, tanto para backup/arquivamento em disco quanto para a movimentação/replicação de dados desduplicados, independentemente do número de dispositivos de armazenamento que compõem a infraestrutura da CONTRATANTE.

3.31.2. A solução deverá implementar desduplicação a nível de blocos, não sendo aceita a técnica de Single-Instance Storage.

3.31.3. Deverá implementar desduplicação de blocos na origem (*client-side deduplication*), de forma que o cliente envie apenas os novos blocos de dados criados e/ou modificados a partir do último backup completo.

3.31.4. Deverá implementar desduplicação de dados nos servidores de armazenamento (target deduplication), de forma que esses servidores tratem adequadamente os blocos repetidos enviados pelos clientes, evitando o armazenamento de blocos redundantes.

3.31.5. Deverá implementar desduplicação de dados global, garantindo que o backup/arquivamento de determinado arquivo ocorra apenas uma vez, independentemente do site ou localidade de origem. A desduplicação global deverá ocorrer em uma única área de armazenamento.

3.31.6. Deverá implementar desduplicação de dados em *jobs* de backup.

3.31.7. Deverá implementar desduplicação de dados em j*obs* de arquivamento.

3.31.8. Deverá implementar desduplicação e compressão em um mesmo *job*.

3.31.9. Deverá permitir o restore granular de arquivos ou sistemas de arquivos a partir de backups em disco ou fita. Em caso de backup armazenado em disco, o *restore* granular poderá ser realizado utilizando backups que estejam desduplicados.

3.31.10. A solução deverá garantir a imutabilidade do armazenamento do backup, assegurando que, em caso de ataque cibernético, o repositório de backup esteja protegido.

## 3.32. SOLUÇÃO DE SNAPSHOT

3.32.1. A solução de backup deverá possuir integração com a funcionalidade de snapshot dos subsistemas de armazenamento em disco, permitindo:

3.32.1.1. Gerenciamento dos snapshots.

3.32.1.2. Registro dos snapshots na base relacional de catálogos, possibilitando buscas por snapshots.

3.32.1.3. Controle do período de validade dos snapshots, realizando a expiração automática assim que o período de retenção configurado seja atingido.

3.32.1.4. A integração com os snapshots deverá ser realizada via API, não sendo aceitos scripts manuais de pré e pós-backup para essa funcionalidade.

3.32.1.5. Efetuar uma cópia dos snapshots criados para disco com desduplicação.

## 3.33. PROTEÇÃO CONTRA RANSOMWARE

3.33.1. A solução deverá oferecer proteção contra Ransomware, implementando as seguintes funcionalidades:

3.33.1.1. Capacidade de implementar Ambiente de Recuperação Isolado e tecnologia Air-gap.

3.33.1.2. Capacidade de criação de cópia de backup imutável.

3.33.1.3. Capacidade de criação de cópia de backup WORM (Write Once, Read Many).

3.33.1.4. Capacidade de detecção de Ransomware (alteração de arquivos), baseada em análise comportamental no ambiente de produção.

## 3.34 SERVIÇO DE MOVIMENTAÇÃO DE DADOS

3.34.1 CARACTERÍSTICAS GERAIS DO SERVIÇO DE MOVIMENTAÇÃO DE DADOS

3.34.1.1. O servidor deverá atender às seguintes especificações:

3.34.1.2. Possuir 1 (um) processador físico padrão x86, no mínimo Intel Xeon Gold 5416S. Cada processador deverá ter, no mínimo, 16 (dezesseis) núcleos físicos, 32 (trinta e dois) threads, 30 MB (trinta megabytes) de cache, suportar instrução de 64 bits, frequência base de 2,0 GHz (dois gigahertz) e frequência turbo máxima de 4,0 GHz (quatro gigahertz).

3.34.1.3. Possuir 64 GB de memória RAM DDR5 ECC.

3.34.1.4. Possuir, no mínimo, 02 (dois) discos de estado sólido (SSD) de, no mínimo, 1,92 TB (uma vírgula noventa e dois terabytes), padrão SAS ou SATA de 6,0 Gb/s, ou superior.

3.34.1.5. Possuir, no mínimo, 04 (quatro) discos mecânicos (HDD) de, no mínimo, 4 TB (quatro terabytes), padrão SAS ou SATA de 6,0 Gb/s, ou superior.

3.34.1.6. Possuir ao menos 4 (quatro) portas 1 GbE RJ-45.

3.34.1.7. Possuir uma porta Gigabit Ethernet padrão 1000Base-T dedicada ao módulo de gerenciamento IPMI ou similar.

3.34.1.8. Possuir uma porta VGA.

3.34.1.9. Possuir duas portas USB 3.0.

3.34.1.10. No painel frontal do chassi, possuir botão de energia e luzes indicativas de alertas.

3.34.1.11. Deverá vir acompanhado de licenças Microsoft Windows Datacenter Standard para toda a capacidade dos servidores.

3.34.1.12. A solução deverá ser certificada pelo INMETRO ou correspondente.

## 3.35. SERVIÇO DE MOVIMENTAÇÃO DE DADOS

### 3.35.1. CARACTERÍSTICAS GERAIS DO SERVIÇO DE MOVIMENTAÇÃO DE DADOS

3.35.2. O servidor deverá atender às seguintes especificações:

3.35.3. Possuir 1 (um) processador físico padrão x86, no mínimo Intel Xeon Gold 5416S. Cada processador deverá ter, no mínimo, 16 (dezesseis) núcleos físicos, 32 (trinta e dois) threads, 30 MB (trinta megabytes) de cache, suportar instruções de 64 bits, frequência base de 2,0 GHz (dois gigahertz) e frequência turbo máxima de 4,0 GHz (quatro gigahertz).

3.35.4. Possuir 64 GB de memória RAM DDR5 ECC.

3.35.5. Possuir, no mínimo, 02 (dois) discos de estado sólido (SSD) de, no mínimo, 1,92 TB (um vírgula noventa e dois terabytes), padrão SAS ou SATA de 6,0 Gb/s, ou superior.

3.35.6. Possuir, no mínimo, 04 (quatro) discos mecânicos (HDD) de, no mínimo, 4 TB (quatro terabytes), padrão SAS ou SATA de 6,0 Gb/s, ou superior.

3.35.7. Possuir ao menos 4 (quatro) portas 1 GbE RJ-45.

3.35.8. Possuir uma porta Gigabit Ethernet padrão 1000Base-T dedicada ao módulo de gerenciamento IPMI ou similar.

3.35.9. Possuir uma porta VGA.

3.35.10. Possuir duas portas USB 3.0.

3.35.11. No painel frontal do chassi, possuir botão de energia e luzes indicativas de alertas.

3.35.12. Deverá vir acompanhado de licenças Microsoft Windows Datacenter Standard para toda a capacidade dos servidores.

3.35.13. A solução deverá ser certificada pelo INMETRO ou por órgão correspondente.

## 3.36. SERVIÇO DE TRANSBORDO DE CÓPIAS DE SEGURANÇA – TIPO QUENTE

### 3.36.1 CARACTERÍSTICAS GERAIS DO SERVIÇO DE TRANSBORDO DE CÓPIAS DE SEGURANÇA – TIPO QUENTE

3.36.1.1. Deverá ser fornecido um serviço de armazenamento externo conforme a descrição abaixo:

3.36.1.2. O sistema de armazenamento deve ser constituído por, no mínimo, 02 (duas) controladoras de discos, operando em modo cluster, sem ponto único de falha, de modo a garantir total disponibilidade, com "failover" automático.

3.36.1.3. O equipamento deverá ser novo, em linha de produção e constar no catálogo do fabricante. Não serão aceitos equipamentos usados, remanufaturados, de demonstração ou montados exclusivamente para este certame.

3.36.1.4. Todos os requisitos da contratação devem ser entregues licenciados, e termos como "deve", "permite", "suporta", "efetua", "proporciona" e "possui" indicam que a funcionalidade deve ser entregue operacional, sem ônus adicional à CONTRATANTE.

3.36.1.5. Deverá ser fornecido um sistema de armazenamento de dados (Storage) do tipo unificado, sem utilização de gateways, com suporte simultâneo aos protocolos S3, CIFS, NFS, iSCSI e FC.

3.36.1.6. A arquitetura do storage não deve ter ponto único de falha, de forma que a falha de qualquer componente não impeça o funcionamento completo do sistema, devendo permitir substituição de componentes defeituosos sem interrupção dos serviços, e as falhas devem ser imperceptíveis aos usuários finais.

3.36.1.7. O sistema deverá permitir manutenção, reparo, substituição e acréscimo de componentes, como controladoras, discos (exceto novas enclosures), fontes e ventiladores, com o sistema em operação, ou seja, os componentes devem ser "Hot Swappable".

3.36.1.8. Deverá haver suporte para failover automático da controladora e mecanismo de proteção de cache em caso de falha de energia ou qualquer outro componente do storage.

3.36.1.9. A solução deve suportar discos SAS, NL-SAS e SSD.

3.36.1.10. A solução deverá permitir expansão para, no mínimo, 144 (cento e quarenta e quatro) discos no mesmo par de controladoras.

3.36.1.11. A solução deverá suportar, no mínimo, 2 PB (dois petabytes) de discos brutos instalados no storage ofertado (único par de controladoras), com a adição de gavetas e discos (crescimento scale-up).

3.36.1.12. Não será permitida a utilização de gateways NAS para prover os protocolos CIFS e NFS.

3.36.1.13. Deverá ser possível implementar discos "Global Hot-Spare" por controladora, de forma que o disco hot-spare sirva como substituto automático, sem intervenção humana, para qualquer disco que venha a falhar. O disco avariado deverá ser substituído sem interrupção do storage ou da aplicação que está acessando o Array.

3.36.1.14. A solução de armazenamento deverá possuir, no mínimo, 64 GB (sessenta e quatro gigabytes) de memória cache instalada e ativa para SAN e NAS, distribuída igualmente no par de controladoras.

3.36.1.14.1. Serão aceitas apenas tecnologias baseadas em memória RAM. Não serão aceitas tecnologias de expansão baseadas em discos SSD/NMVe ou módulos PCIe.

3.36.1.15. O sistema de armazenamento deverá possuir a seguinte composição de portas de front-end ativas:

3.36.1.16. 8 (oito) portas 1/10 Gbps Ethernet para CIFS, iSCSI e NFS, padrão Base-T RJ-45.

3.36.1.16.1. Deverá ser compatível com os protocolos Ethernet solicitados (iSCSI, NFS e SMB). Caso o equipamento tenha alguma restrição de utilização simultânea de todos os protocolos na mesma porta, deverão ser entregues 04 (quatro) portas para cada tipo de protocolo.

3.36.1.17. O sistema de armazenamento deverá possuir, no mínimo, 04 (quatro) portas de back-end operando a, no mínimo, 12 Gbit/s.

3.36.1.18. A solução deverá permitir crescimento horizontal (scale-out) com equipamentos do mesmo fabricante, mesmo que de modelos diferentes, dentro de uma mesma solução em modo cluster, com no mínimo as seguintes funcionalidades:

3.36.1.19. Permitir a expansão para até, no mínimo, 12 (doze) nós de cluster, atendendo às camadas SAN e NAS.

3.36.1.20. O equipamento de armazenamento deverá possuir fontes de alimentação elétrica bivolt (110/220 VAC) redundantes.

## 3.37. ESPECIFICAÇÃO DE VOLUMETRIA

3.37.1. A capacidade de armazenamento deve ser considerada na unidade de Tebibyte (1 Tebibyte = 2^40 bytes = 1.099.511.627.776 bytes = 1.024 Gibibytes).

3.37.2. O serviço de armazenamento de dados deverá possuir uma capacidade de armazenamento mínima de 4 TiB (Quatro Tebibytes) em discos NL-SAS ou superior, de acordo com os critérios definidos neste termo de referência.

3.37.2.1. Define-se como capacidade de armazenamento líquida o total de bytes instalados e disponíveis para o armazenamento de dados, descontados os bytes utilizados pelo software de storage para proteção de RAID, hot-pares, e sem considerar ganhos com deduplicação, compressão ou outros mecanismos de redução de dados.

3.37.3. O tamanho máximo das unidades de disco será:

3.37.3.1. NL-SAS: 10 TB;

3.37.3.2. SAS: 1.8 TB;

3.37.3.3. SSD: 960 GB.

3.37.4. O equipamento deverá fornecer os seguintes níveis de proteção de disco:

3.37.4.1. Paridade Simples (RAID 5 ou similar);

3.37.4.2. Paridade Dupla (RAID 6 ou similar);

3.37.4.3. Paridade Tripla, para discos densos maiores que 8 TB.

## 3.38. FUNCIONALIDADES DA SOLUÇÃO DE PROTEÇÃO DE DADOS

3.38.1. O sistema operacional do sistema de armazenamento de dados deverá ser nativo do produto, não sendo permitidas modalidades OEM de sistemas operacionais de uso genérico, como Windows e suas variações ou Unix/Linux e suas variações.

3.38.2. O sistema deverá suportar os seguintes protocolos:

3.38.2.1. Na modalidade SAN (Storage Area Network): iSCSI e FCP (Fibre Channel Protocol).

3.38.2.2. Na modalidade NAS (Network Attached Storage): CIFS (Common Internet File System) versão 2.0 e superiores, NFS (Network File System) versão 3 e superiores, e NDMP (Network Data Management Protocol) versão 4 e superiores.

3.38.2.3. Na modalidade Objeto: S3.

3.38.2.4. A implementação das arquiteturas SAN (iSCSI e FCP), NAS (CIFS e NFS) e Objeto (S3) deverá ser nativa ao produto, garantindo total compatibilidade.

3.38.3. Deverá permitir a criação de, pelo menos, 16.000 LUNs por par de controladoras.

3.38.4. A solução de armazenamento deverá permitir o acesso simultâneo aos dados de um mesmo volume por meio dos protocolos CIFS e NFS.

3.38.5. O array deverá implementar mecanismos de proteção (LUN masking) entre volumes, de forma que sejam visíveis ou utilizáveis apenas pelos hosts destinados.

3.38.6. Deverá permitir a utilização de múltiplos caminhos ativos e balanceados para o mesmo servidor acessar as LUNs, utilizando o recurso de Multipath/MPIO.

3.38.7. Deverá permitir o acesso às LUNs a partir de qualquer porta de front-end, utilizando software de multipath nativo dos sistemas operacionais descritos neste edital.

3.38.8. Deverá permitir a implementação das funções de agregação de portas (trunking) e VLAN, conforme padrões IEEE 802.3ad e IEEE 802.1Q, com suporte a Jumbo Frames nas interfaces Ethernet.

3.38.9. Deverá possuir monitoramento proativo que permita a detecção e isolamento de falhas antes que ocorram, abrangendo desde a auto monitoração, geração de log de erros, detecção e isolamento de erros de memória e de disco, incluindo o acionamento automático de disco de reposição (disk spare) e a funcionalidade de call-home.

3.38.10. Deverá possuir a função de call-home por meio de linha telefônica comum, e-mail ou VPN (Virtual Private Network) para diagnóstico remoto em caso de erros ou defeitos.

3.38.11. O sistema de armazenamento deverá fornecer níveis de proteção de disco:

3.38.11.1. Paridade Simples (RAID 5 ou similar).

3.38.11.2. Paridade Dupla (RAID 6 ou similar).

3.38.11.3. Paridade Tripla para discos densos maiores que 8 TB.

3.38.12. Deverá ser fornecida com a funcionalidade de snapshot ou point-in-time backup de quaisquer áreas de dados (volume/partição) da solução, com capacidade para armazenar, no mínimo, 1.023 versões por volume/partição. Essa funcionalidade deverá ser executada internamente à solução, sem consumir ciclos de CPU dos sistemas clientes conectados e sem gerar movimentação de dados.

3.38.13. Deverá contemplar a funcionalidade de restore de volumes ou arquivos, permitindo a restauração utilizando os pontos de consistência (snapshots ou clones) previamente gerados, inclusive com restore granular de volumes ou arquivos.

3.38.14. Deverá ser fornecida com a funcionalidade de criar cópias clone independentes dos dados originais, permitindo a transformação em um novo volume lógico a qualquer momento.

3.38.15. Deverá suportar o provisionamento virtual da capacidade (thin provisioning) de volumes ou partições lógicas.

3.38.16. Deverá permitir o redimensionamento imediato do tamanho dos volumes/LUNs sem impacto ou reconfiguração para os clientes.

3.38.17. Deverá permitir a execução da função de servidor de arquivos diretamente no sistema de armazenamento para clientes NAS, sem a necessidade de controladoras adicionais.

3.38.18. Deverá suportar controle de quotas por usuários e pastas no ambiente NAS.

3.38.19. Deverá possuir capacidade de gerenciar o acesso simultâneo de usuários CIFS e NFS (File Locking).

3.38.20. Deverá permitir auditoria dos arquivos gravados via protocolos CIFS, com gerenciamento on-line.

3.38.21. Deverá permitir integração com o Active Directory (AD) Microsoft e gerenciamento de segurança por Access Control Lists (ACLs) integrados ao AD.

3.38.22. A solução deverá permitir a definição de diferentes configurações de segurança em cada nível de diretório dos compartilhamentos configurados no NAS.

3.38.23. Deverá possuir a funcionalidade de Access Based Enumeration (ABE) para o ambiente Windows com acesso via protocolo CIFS.

3.38.24. Deverá possuir recurso de filtro de arquivos por extensão.

3.38.25. Deverá suportar VMware vSphere API for Array Integration (VAAI), VMware vStorage APIs for Storage Awareness (VASA), VMware vCenter Site Recovery Manager (SRM) e VMware Virtual Volume (VVOL).

3.38.26. Deverá possuir plug-in para integração com o vCenter (VMware), permitindo configurar políticas de acesso e visualização de informações do subsistema de armazenamento.

3.38.27. Deverá contemplar a funcionalidade de desduplicação para volumes SAN e NAS.

3.38.28. Deverá contemplar a funcionalidade de compressão para volumes SAN e NAS.

3.38.29. A solução deverá permitir o gerenciamento de qualidade de serviço (QoS) para definir o limite de IOPs e/ou MB/s em nível de arquivos, volumes e LUNs.

3.38.30. Deverá suportar replicação assíncrona e síncrona de sistemas de arquivos (NAS) e LUNs (SAN) para sistemas de armazenamento do mesmo fabricante.

## 3.39. INTEGRAÇÃO COM APLICAÇÕES

3.39.1. Deverá ser fornecido com os softwares/licenças para integração com as seguintes aplicações:

3.39.1.1. Gerenciadores de bancos de dados: Microsoft SQL Server.

3.39.1.2. Sistemas e serviços: Microsoft Exchange e Microsoft Cluster Service.

3.39.1.3. Sistemas operacionais: VMware ESX, Microsoft Windows Server, Linux Red Hat.

3.39.1.4. Virtualizadores: VMware e Microsoft Hyper-V.

3.39.2. A integração, de acordo com a aplicação, deverá controlar pelo menos a criação de snapshots e recuperação de backups via snapshot.

3.39.3. Deverá permitir a geração, por interface gráfica, de snapshots íntegros, restore e espelhamento de máquinas virtuais.

## 3.40. SOFTWARE DE GERENCIAMENTO

3.40.1. Possuir software de gerenciamento centralizado com as seguintes funcionalidades:

3.40.1.1. Definição de áreas de acesso para os clientes, análise de performance, determinação de problemas, monitoração do uso e desempenho do sistema de entrada/saída e utilização dos demais recursos do servidor de armazenamento.

3.40.1.2. Controle e análise de capacidade e configuração dos parâmetros físicos e lógicos do subsistema de armazenamento.

3.40.1.3. Deve permitir estabelecimento de níveis de acesso por usuário baseado no seu perfil de trabalho e responsabilidades.

3.40.1.4. Alocação dinâmica dos volumes lógicos das unidades entre os servidores.

3.40.1.5. Correlação de eventos e diagnóstico de performance.

3.40.1.6. Interface de gerenciamento gráfica e/ou Web, com controle de acesso seguro via HTTPS e SSH.

3.40.1.7. Notificação de eventos críticos, possibilitando uma administração proativa.

3.40.1.8. Gerenciamento dos "RAID GROUPS" em diversas plataformas.

3.40.1.9. Monitoramento proativo que permita a detecção e isolamento de falhas até mesmo antes que elas ocorram, abrangendo auto monitoração, geração de log de erros, detecção e isolamento de erros de memória e de discos, incluindo acionamento automático de disco de spare.

3.40.1.10. Permitir o gerenciamento com provisionamento de crescimento do sistema.

3.40.1.11. Apresentação de um conjunto de informações gerenciais acessíveis em smartphone via app específico IOS/Android e via Web mobile.

3.40.1.12. Deverá possuir recurso que permita monitorar graficamente e armazenar estatísticas da capacidade e do desempenho do Sistema, com histórico de dados de no mínimo 6 (seis) meses.

3.40.1.12.1. Caso o Sistema necessite de recursos externos para preencher esse requisito, o mesmo deverá incluir todos os componentes necessários, como servidores, licenças de sistema operacional, licença de software, entre outros. Em possibilidade de utilização de máquina virtual, o recurso de processamento e virtualização será provido pelo CONTRATANTE.

## 3.41. COMPATIBILIDADE

3.41.1. A solução deverá ser compatível com:

3.41.1.1. Deverá suportar os protocolos iSCSI e FCP para os ambientes operacionais com VMware ESX, Red Hat Linux, SuSE Linux e Microsoft Windows via Microsoft-Logo Certified, constando na HCL da Microsoft.

3.41.2. Deverá ser comprovado via site do fabricante.

3.41.2.1. Deverá ser compatível com softwares de antivírus externos para executar varreduras no ambiente de armazenamento NAS, como McAfee, Sophos, Symantec e Trend Micro.

## 3.42. REQUISITOS DE SEGURANÇA

3.42.1. A solução deverá suportar a funcionalidade MFA (Multi-Factor Authentication), ou seja, deve ser possível tanto para acesso web quanto para acesso CLI que o usuário tenha acesso ao storage somente após apresentar com sucesso duas ou mais evidências para um mecanismo de autenticação, como um token. Caso a solução não apresente tal funcionalidade, será aceito um jump host para realizar o provedor de autenticação.

3.42.1.1. A solução deverá possuir verificação Multi-Admin, permitindo que certas tarefas necessitem da autorização de dois ou mais administradores, prevenindo que alterações indesejadas sejam executadas.

3.42.2. O subsistema deverá possuir software para criptografia dos dados com as seguintes funcionalidades:

3.42.2.1. Deverá possuir tecnologia nativa para criptografia dos dados armazenados no subsistema, utilizando algoritmo AES-256 ou superior.

3.42.2.2. A funcionalidade deverá ser totalmente nativa ao subsistema, sem necessidade de hardware ou software externo para a gerência da(s) chave(s) de criptografia ou qualquer outra rotina relacionada à cifragem dos dados. Caso haja necessidade, a proponente deve considerar o servidor e a licença necessária para tal funcionalidade.

3.42.2.3. A funcionalidade deverá estar licenciada para a capacidade máxima total suportada pelo subsistema definido neste termo.

3.42.2.4. O subsistema deverá permitir a coexistência de dados cifrados e não cifrados no mesmo subsistema.

3.42.2.5. O subsistema deverá permitir a ativação e o desligamento da funcionalidade, em nível de LUN ou volume, a qualquer tempo.

3.42.2.6. O subsistema deverá suportar a implementação da funcionalidade de criptografia para as áreas NAS (CIFS e NFS) e SAN (FC e iSCSI).

3.42.2.7. Caso o subsistema não possua tal funcionalidade, o subsistema deverá ser fornecido com garantia do tipo “Non-Returnable Disk”, que cobre a substituição de discos defeituosos sem que a CONTRATANTE retorne os dispositivos falhados.

3.42.2.8. A garantia do tipo “Non-Returnable Disk” deverá perdurar durante todo o período de garantia especificado neste caderno técnico.

3.42.2.9. Na assinatura do contrato, será exigido certificado do fabricante que comprove o fornecimento de tal garantia.

3.42.2.10. Deverá possuir conformidade com FIPS 140-2. Federal Information Processing Standard (FIPS) Publication 140 é um padrão que define requisitos mínimos de segurança para módulos criptográficos em produtos e sistemas.

3.42.2.10.1. A comprovação da conformidade com a FIPS 140-2 será validada em: FIPS 140-2 validation.

3.42.3. Deverá possuir funcionalidade e ser licenciado para utilização do WORM (Write Once, Read Many).

3.42.4. Deverá possuir funcionalidade de detecção e prevenção de ataques ransomware.

3.42.4.1.1. A funcionalidade deve usar análise de carga de trabalho em ambientes NAS (NFS e SMB) para detectar e alertar proativamente sobre atividades anormais que possam indicar um ataque de ransomware.

3.42.4.1.2. Em casos de suspeita de um ataque, a funcionalidade deverá ser capaz de acionar uma resposta automática através de snapshot ou similar, para mitigar os danos da possível infecção.

3.42.4.1.3. Caso a solução ofertada não possua a respectiva funcionalidade de forma nativa, a solução poderá ser composta com produtos de terceiros para atendimento deste requisito para a capacidade total de armazenamento solicitada.

## 3.43. SERVIÇO DE CONECTIVIDADE

### 3.43.1 CARACTERÍSTICAS SOLUÇÃO DE CONECTIVIDADE

3.43.1.1. Possuir homologação da ANATEL. O certificado do equipamento deve estar válido na data de abertura desse processo para fins de comprovação do item.

3.43.1.2. A solução deve ser composta de um único equipamento, montável em rack 19”, devendo este vir acompanhado dos devidos acessórios para tal.

3.43.1.3. Possuir altura máxima de 1U (1,75").

3.43.1.4. Implementar jumbo frames em todas as portas ofertadas, com suporte a frames de até 9216 bytes.

3.43.1.5. Implementar Port Isolation ou funcionalidade que permita isolamento de portas específicas do switch.

3.43.1.6. Implementar detecção de oscilação (flap) de links, permitindo desabilitar uma porta caso a porta oscile acima de um limiar configurado.

3.43.1.7. Suportar agregação de links conforme padrão IEEE 802.3ad ou 802.1AX com, no mínimo, 8 grupos, sendo 8 links agregados por grupo.

3.43.1.8. A Memória Flash instalada deve ser suficiente para comportar, no mínimo, duas imagens do Sistema Operacional simultaneamente, permitindo que seja feito um upgrade de Software e a imagem anterior seja mantida.

3.43.1.9. Implementar Port Isolation ou funcionalidade que permita isolamento de portas específicas do switch. As portas isoladas não devem se comunicar entre si, porém podem se comunicar com qualquer outra porta no equipamento que não esteja isolada.

3.43.1.10. Implementar detecção de oscilação (flap) de links, permitindo desabilitar uma porta caso a porta oscile acima de um limiar configurado.

3.43.1.11. Implementar 4000 VLANs ativas simultaneamente, através do protocolo 802.1Q.

3.43.1.12. Deverá permitir a criação de VLANs e adição de portas a VLANs de forma dinâmica através do protocolo MVRP, segundo o padrão IEEE802.1ak.

3.43.1.13. Possibilitar a coleta de estatísticas de tráfego baseada em VLANs IEEE 802.1Q e double-tagged VLANs IEEE 802.1ad.

3.43.1.14. Implementar VLAN Translation.

3.43.1.15. Implementar Private VLANs.

3.43.1.16. Implementar VLAN Aggregation ou funcionalidade que permita o compartilhamento de uma mesma subnet e de um mesmo endereço IPv4 utilizado como default-gateway por hosts de diferentes VLANs.

3.43.1.17. Implementar MAC Based VLAN.

3.43.1.18. Implementar Proxy-ARP (RFC 1027).

3.43.1.19. Implementar IGMP v1, v2 e v3 Snooping.

3.43.1.20. Implementar IGMPv1 (RFC 1112), IGMP v2 (RFC 2236) e IGMPv3 (RFC 3376).

3.43.1.21. Implementar MVR (Multicast VLAN Registration).

3.43.1.22. Implementar DHCP/Bootp relay configurável por VLAN para IPv4 e IPv6.

3.43.1.23. Implementar servidor DHCP interno que permita a configuração de um intervalo de endereços IP a serem atribuídos aos clientes DHCP, e possibilite ainda a atribuição de, no mínimo, default gateway, servidor DNS e servidor WINS.

3.43.1.24. Implementar DHCP Option 82, de acordo com a RFC 3046, com identificação de porta e VLAN.

3.43.1.25. Implementar DHCP Client para IPv4 e IPv6.

3.43.1.26. Implementar IEEE 802.1ab Link Layer Discovery Protocol (LLDP).

3.43.1.27. Implementar LLDP-MED (Media Endpoint Discovery).

3.43.1.28. Implementar Spanning-Tree (IEEE 802.1d), Rapid Spanning Tree (IEEE 802.1w), Multiple Instance STP (802.1s) e PVST+.

3.43.1.29. Implementar a configuração de Multiple Spanning Tree Protocol, com suporte a, no mínimo, 16 domínios.

3.43.1.30. Implementar o protocolo ITU-T G.8032 ERPS.

3.43.1.31. Implementar L2 ping e L2 traceroute, conforme IEEE 802.1ag (Connectivity Fault Management).

3.43.1.32. Implementar funcionalidade baseada na recomendação do ITU-T Y.1731 com medição de, no mínimo, Frame Delay.

3.43.1.33. Implementar prefixos IPv4 de 31 bits, conforme RFC 3021.

3.43.1.34. Implementar roteamento estático com suporte a, no mínimo, 32 rotas.

3.43.1.35. Implementar Dual Stack, ou seja, IPv6 e IPv4, com suporte às seguintes funcionalidades/RFCs:

3.43.1.35.1. RFC 1981, Path MTU Discovery for IPv6.

3.43.1.35.2. RFC 5095, Internet Protocol, Version 6 (IPv6) Specification.

3.43.1.35.3. RFC 4861, Neighbor Discovery for IP Version 6 (IPv6).

3.43.1.35.4. RFC 2462, IPv6 Stateless Address Autoconfiguration.

3.43.1.35.5. RFC 2463, Internet Control Message Protocol (ICMPv6) for the IPv6 Specification.

3.43.1.35.6. RFC 2464, Transmission of IPv6 Packets over Ethernet Networks.

3.43.1.35.7. RFC 2465, IPv6 MIB, General Group and Textual Conventions.

3.43.1.35.8. RFC 2466, MIB for ICMPv6.

3.43.1.35.9. RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture.

3.43.1.35.10. RFC 3587, Global Unicast Address Format.

3.43.1.36. Deve implementar as seguintes RFCs relacionadas a IPv6:

3.43.1.36.1. RFC 2710, Multicast Listener Discovery v1 (MLDv1).

3.43.1.36.2. RFC 3810, Multicast Listener Discovery v2 (MLDv2).

3.43.1.37. Implementar PIM Snooping.

3.43.1.38. Implementar gerenciamento através de SNMPv1 (RFC 1157), v2c (RFCs 1901 a 1908), e v3 (RFCs 3410 a 3415).

3.43.1.39. Implementar ajuste de relógio (clock) do equipamento utilizando NTP com autenticação MD5, e SNTP.

3.43.1.40. Possuir cliente DNS para IPv4, segundo a RFC 1591, e cliente DNS para IPv6.

3.43.1.41. Possuir cliente e servidor Telnet, segundo a RFC 854.

3.43.1.42. Implementar cliente e servidor SSHv2.

3.43.1.43. Implementar a atualização de imagens de software e configuração através de um servidor TFTP.

3.43.1.44. Implementar cliente e servidor SCP e servidor SFTP.

3.43.1.45. Implementar upload e download de configuração em formato ASCII ou XML, permitindo a edição do arquivo de configuração e, posteriormente, o download do arquivo editado para o equipamento.

3.43.1.46. Suportar envio de logs para múltiplos servidores Syslog.

3.43.1.47. Implementar TACACS+ segundo a RFC 1492, não sendo aceitos protocolos similares.

3.43.1.48. Implementar autenticação RADIUS com suporte a:

3.43.1.48.1. RFC 2865, RADIUS Authentication.

3.43.1.48.2. RFC 2866, RADIUS Accounting.

3.43.1.48.3. RFC 3579, RADIUS EAP support for 802.1X.

3.43.1.49. Implementar RADIUS sobre TLS (RadSec).

3.43.1.50. A implementação de RADIUS deve suportar alteração dinâmica de parâmetros de autorização de uma sessão já ativa.

3.43.1.51. A implementação de RADIUS e TACACS+ deve estar disponível para autenticação de usuários de gerenciamento do equipamento.

3.43.1.52. Implementar per-command authentication para RADIUS.

3.43.1.53. Implementar os seguintes grupos de RMON através da RFC 1757 ou RFC 2819: History, Statistics, Alarms e Events.

3.43.1.54. Implementar sFlow ou Netflow.

3.43.1.55. Implementar os seguintes protocolos em IPv6: Ping, Traceroute, Telnet, SSHv2, DNS e RADIUS.

3.43.1.56. Implementar gerenciamento via web.

3.43.1.57. A interface gráfica deve permitir visualização de informações do sistema, monitoramento de eventos, utilização de portas e permitir configuração de VLANs e ACLs.

3.43.1.58. O sistema operacional deve possuir função grep/pipe para filtrar a saída de determinado comando.

3.43.1.59. O sistema operacional deve possuir comandos para visualização e monitoração de cada processo, sendo possível verificar por processo qual o consumo de CPU, process-id e qual o consumo de memória por processo.

3.43.1.60. O sistema operacional deve possuir comandos para que processos sejam terminados ou reiniciados sem a necessidade de reinicialização do equipamento. Esta funcionalidade deve estar disponível para, no mínimo, Telnet, TFTP, HTTP e LLDP na versão atual.

3.43.1.61. Implementar linguagem de scripting baseada em Python, permitindo a automatização de tarefas. A linguagem deve implementar estruturas de controle como loops e execução condicional e permitir a definição de variáveis.

3.43.1.62. Deve disponibilizar API (Application Programming Interface) aberta para integração com aplicações.

3.43.1.63. A funcionalidade de Rate Shaping deve permitir a configuração de CIR (Commited Rate) e peak rate.

3.43.1.64. Implementar a leitura, classificação e remarcação de QoS (802.1p e DSCP).

3.43.1.65. Implementar remarcação de prioridade de pacotes Layer 3, remarcando o campo DiffServ para grupos de tráfego classificados segundo portas TCP e UDP, endereço/sub-rede IP, VLAN e MAC origem e destino.

3.43.1.66. Implementar 8 filas de prioridade em hardware por porta.

3.43.1.67. Implementar os algoritmos de gerenciamento de filas WRR (Weighted Round Robin), WDRR (Weighted Deficit Round Robin) e SP (Strict Priority).

3.43.1.68. Implementar as seguintes RFCs relacionadas a DiffServ: RFC 2474, RFC 2597 e RFC 2598.

3.43.1.69. Implementar classificação de tráfego para QoS de camada 2 e camada 3 baseada em MAC, IP, porta, DiffServ e 802.1p.

3.43.1.70. Implementar funcionalidade que permita que somente servidores DHCP confiáveis atribuam endereço IP aos clientes DHCP (Trusted DHCP Server).

3.43.1.71. Implementar Gratuitous ARP Protection.

3.43.1.72. Implementar detecção e proteção contra-ataques Denial of Service (DoS) direcionados à CPU do equipamento.

3.43.1.73. Implementar limitação de número de endereços MAC aprendidos por uma porta. Deve permitir desabilitar a porta caso a quantidade de endereços MAC ultrapasse o limite configurado.

3.43.1.74. Implementar travamento de endereços MAC, permitindo a adição estática de endereços para uma determinada porta ou utilizando os endereços existentes na tabela MAC.

3.43.1.75. Implementar login de rede baseado no protocolo IEEE 802.1X, permitindo que a porta do switch seja associada à VLAN definida para o usuário no servidor RADIUS.

3.43.1.76. A implementação do IEEE 802.1X deve incluir suporte a Guest VLAN, encaminhando o usuário para esta VLAN caso este não possua suplicante 802.1X ativo.

3.43.1.77. Implementar múltiplos suplicantes por porta, onde cada dispositivo deve ser autenticado de forma independente, podendo ser encaminhados a VLANs distintas. As múltiplas autenticações devem ser realizadas através de IEEE 802.1X.

3.43.1.78. Implementar autenticação baseada em web, com suporte a SSL, através de RADIUS ou da base local do switch.

3.43.1.79. Implementar autenticação baseada em endereço MAC.

3.43.1.80. Implementar ACLs de entrada (ingress ACLs) em hardware, baseadas em critérios da camada 2 (MAC origem e destino e campo 802.1p), camada 3 (IP origem e destino) e camada 4 (portas TCP e UDP).

3.43.1.81. As ACLs devem implementar as seguintes ações: permitir, negar, aplicar QoS, espelhar o tráfego para uma porta de análise, criar entrada de log e incrementar contador.

3.43.1.82. Implementar funcionalidade que permita a execução de ACLs em um determinado horário do dia.

3.43.1.83. Implementar políticas por usuário, permitindo que as configurações de ACL e QoS sejam aplicadas na porta utilizada para a conexão à rede, após a autenticação.

3.43.1.84. Implementar funcionalidade que permita a detecção de telefones VoIP, de forma automática, que utilizem o protocolo CDP ou LLDP, e permitir a aplicação dinâmica de políticas de segurança na porta do switch com base no dispositivo detectado.

## 3.44. CARACTERÍSTICAS ESPECÍFICAS DO SERVIÇO DE CONECTIVIDADE

### 3.44.1 SWITCH

3.44.1.1. Deverá ser fornecido um switch com, no mínimo, a seguinte configuração:

3.44.1.1.1. Possuir, no mínimo, 24 portas 10/100/1000BASE-T, baseadas em RJ-45, com suporte a PoE padrão 802.3at, com suporte de, no mínimo, 30W por porta.

3.44.1.1.2. Possuir, no mínimo, 4 portas uplink de 100M/1/2.5GBASE-X SFP, adicionais às portas solicitadas anteriormente.

3.44.1.1.3. O equipamento deve possuir, no mínimo, 370W de potência disponível (budget) para distribuição entre suas portas PoE através de fonte interna.

3.44.1.1.4. Possuir, no mínimo, uma porta de console com conector RJ-45 ou USB Mini-B ou USB Micro-B. Em caso de porta de console USB, deverá permitir sua conexão diretamente à porta USB de um computador, sem conversores externos.

3.44.1.1.5. Possuir, no mínimo, uma porta USB tipo A para usos diversos.

3.44.1.1.6. Possuir, no mínimo, 1 porta 10/100/1000 para gerenciamento out-of-band.

3.44.1.1.7. Possuir LEDs indicativos de funcionamento da fonte de alimentação, ventiladores, status do sistema e atividade das portas de dados.

3.44.1.1.8. Possuir fonte de alimentação interna e redundante que trabalhe em 110V e 220V, 50/60 Hz, com detecção automática de tensão e frequência.

3.44.1.1.9. Caso o equipamento possua ventiladores para refrigeração, o sentido de fluxo deverá ser da frente para trás (front-to-back) ou de um lado para outro (side-to-side).

3.44.1.1.10. Suportar temperatura de operação entre 0 e 45 graus Celsius.

3.44.1.1.11. Suportar capacidade agregada de switching de, no mínimo, 60 Gbps.

3.44.1.1.12. Suportar capacidade de encaminhamento de pacotes de, no mínimo, 50 Mpps utilizando pacotes de 64 bytes.

3.44.1.1.13. Suportar o armazenamento de, no mínimo, 16.000 endereços MAC.

3.44.1.1.14. Suportar o armazenamento de, no mínimo, 32 rotas IPv4 em hardware.

3.44.1.1.15. Suportar o armazenamento de, no mínimo, 15 rotas IPv6 em hardware.

3.44.1.1.16. Implementar, no mínimo, 1.000 regras de ACL de entrada (ingress ACLs).

3.44.1.1.17. Possuir, no mínimo, 512MB de memória RAM com suporte a ECC e 128MB de memória Flash.

3.44.1.1.18. Deverá ser entregue com todos os cabos e acessórios necessários para seu funcionamento.

## 3.45. CARACTERÍSTICAS DOS TRANSCEIVERS

3.45.1. Deve ser fornecido no mínimo 2 unidades de transceiver com o padrão 1000BASE-SX SFP, operando sobre fibras multimodo OM3/OM4 para distâncias de até 1 km.

3.45.2. Deve ser compatível com fibras de 850nm.

3.45.3. Deve permitir a instalação em slots/portas tipo SFP.

3.45.4. Deve possuir conector do tipo LC.

3.45.5. Deve ser do tipo hot-swappable, permitindo sua conexão/desconexão com o equipamento em operação.

3.45.6. Não será aceito o fornecimento de transceiver dito "compatível" que não seja reconhecido pelo fabricante dos equipamentos ou que requeira desabilitar a proteção contra transceivers de terceiros.

3.45.7. Deve ser do mesmo fabricante e totalmente compatível com os switches fornecidos, devendo estar listado na matriz de compatibilidade desses equipamentos.

## 3.46. LICENCIAMENTO DO SWITCH TIPO 1

3.46.1. Deverá realizar a ativação de direito de uso do Switch Tipo 1.

3.46.2. Deverá possuir suporte e garantia associada ao Switch Tipo 1.

3.46.3. O licenciamento deverá ser do tipo perpétuo, de maneira que o equipamento Switch Tipo 1 não perca suas funcionalidades ao término do contrato de suporte e garantia.

## 3.47. CARACTERÍSTICAS DO SOFTWARE DE GERENCIAMENTO DE REDES

3.47.1. Deverá ser do mesmo fabricante dos equipamentos dos switches ofertados. O software de gerenciamento deve ser fornecido em formato local (on-premises), em nuvem pública ou de forma híbrida com ambos trabalhando em conjunto. Em quaisquer das opções ofertadas, a solução deverá ser do mesmo fabricante dos equipamentos deste grupo e deverá seguir os requisitos descritos.

3.47.2. Em caso de componente de nuvem pública:

3.47.3. Deve ser fornecido na modalidade SaaS (Software as a Service) do próprio fabricante. Não será permitida a utilização de softwares instalados em nuvem pública com intuito de atendimento deste termo de referência.

3.47.4. Deve apresentar disponibilidade mínima de 99,9%.

3.47.5. Em caso de componente de solução local (on-premises, através de appliance virtual), deverá ser fornecido em, pelo menos, um dos formatos abaixo:

3.47.6. Hyper-V 2012 R2 ou superior.

3.47.7. VMware vSphere ESXi 6 ou superior.

3.47.8. Deve ser acompanhado de todos os acessórios necessários para operacionalização da solução, tais como: softwares, licenças, documentações técnicas e manuais que contenham informações suficientes, que possibilitem a instalação, configuração e operacionalização do equipamento.

3.47.9. Para atendimento deste termo de referência, será permitida a composição de softwares distintos, desde que sejam do mesmo fabricante para atendimento de toda a especificação.

3.47.10. Deve suportar a centralização da configuração e monitoramento dos switches gerenciados.

3.47.11. Deve suportar o gerenciamento de no mínimo 1.500 switches.

3.47.12. O licenciamento deverá ser considerado de forma unitária, ou seja, cada unidade de licença significa um equipamento, dessa forma será possível gerenciar apenas o número de equipamentos necessários.

3.47.13. Deve permitir o acréscimo unitário de licenças para expansão da capacidade dos switches, e cada switch deve vir acompanhado de sua licença.

3.47.14. As licenças de uso deverão ser na modalidade de subscrição, pelo período de 12 (doze) meses, com garantia, suporte e atualizações, independente da arquitetura adotada (computação virtual ou nuvem pública do fabricante dos switches) para todos os itens que sejam fornecidos para compor a solução.

3.47.15. Implementar, no mínimo, dois níveis de acesso administrativo ao software de gerência (apenas leitura e leitura/escrita).

3.47.16. Permitir a customização do acesso administrativo através de atribuição de grupo de função do usuário administrador.

3.47.17. Permitir a configuração e gerenciamento através de browser padrão (web).

3.47.18. Permitir que o processo de atualização de versão nos dispositivos gerenciados seja realizado através de browser padrão ou SSH.

3.47.19. Possibilitar backup da configuração, bem como a funcionalidade de restauração da configuração e permitir exportar o backup.

3.47.20. Deve permitir fazer o aprovisionamento de switches a partir da sua configuração de fábrica, sem a necessidade de configuração inicial via CLI (Auto-provision, ZTP, etc.).

3.47.21. Deve permitir a criação de políticas ou modelos (templates) de configuração para aplicação a um grupo de switches.

3.47.22. Deve permitir que as configurações sejam aplicadas em vários switches simultaneamente.

3.47.23. Deve permitir que as configurações sejam aplicadas em apenas um switch pontualmente, sobrescrevendo a configuração da política ou modelo (template) de configuração.

3.47.24. Deve permitir a criação e remoção de VLANs nos dispositivos e associação de portas a elas.

3.47.25. Deve permitir a configuração nos switches gerenciados de, no mínimo:

3.47.26. PoE.

3.47.27. LLDP.

3.47.28. SNMP.

3.47.29. NTP ou SNTP.

3.47.30. Syslog.

3.47.31. MTU ou Jumbo Frame.

3.47.32. IGMP Snooping.

3.47.33. STP, RSTP e MSTP.

3.47.34. Limitação de taxa de encaminhamento de broadcast, multicast e unknown unicast, por porta do switch.

3.47.35. Deve permitir a criação de um script ou objeto com comandos de CLI customizados para os dispositivos gerenciados. Deve permitir a aplicação desse script ou objeto para um grupo de dispositivos gerenciados simultaneamente.

3.47.36. Deve permitir acessar os switches utilizando SSH, a partir de conexão com a nuvem.

3.47.37. Deve permitir desabilitar e habilitar as portas dos switches.

3.47.38. Deve permitir monitorar os seguintes parâmetros dos switches:

3.47.39. Utilização de CPU e memória RAM.

3.47.40. Consumo de dados enviados e recebidos, por porta.

3.47.41. Deve permitir visualizar o inventário dos switches, contendo, no mínimo:

3.47.42. Modelo.

3.47.43. Número Serial.

3.47.44. Versão de Software.

3.47.45. Endereço MAC.

3.47.46. Endereço IP.

3.47.47. Deve permitir visualizar informações por porta, contendo, no mínimo:

3.47.48. Status da porta.

3.47.49. VLANs configuradas.

3.47.50. Tráfego enviado e recebido.

3.47.51. Potência PoE fornecida, caso o switch suporte PoE.

3.47.52. Velocidade da porta.

3.47.53. Deverá implementar padrão 802.1Q.

3.47.54. Suportar a configuração de no mínimo 4.000 VLAN IDs.

3.47.55. Deverá implementar DHCP Relay e DHCP Server.

3.47.56. Deve permitir visibilidade e controle das aplicações (camada 7), permitindo, no mínimo, o bloqueio e permissão de aplicações.

3.47.57. Possuir relatório de compliance com regulamentação PCI DSS v3.0 ou superior.

3.47.58. Os itens a seguir devem estar integrados à solução ofertada e não serão aceitos equipamentos externos à solução. Caso sejam necessárias licenças ou softwares de controle, estes devem ser fornecidos de forma que a solução esteja operacional e sem nenhuma restrição no ato de sua implementação (hardware e softwares necessários para implementação).

3.47.59. Implementar, pelo menos, os seguintes controles/filtros:

3.47.60. L2 Baseado em MAC Address de origem e destino.

3.47.61. L3 Baseado em Endereço IP de origem e destino.

3.47.62. Deverá suportar servidor de autenticação RADIUS redundante, isto é, na falha de comunicação com o servidor RADIUS principal, o sistema deverá buscar um servidor RADIUS secundário.

3.47.63. Deverá suportar RADIUS CoA (Dynamic Change of Authorization).

## 3.48. SERVIÇO DE MONITORAMENTO E GERENCIAMENTO DE SOLUÇÕES DE SEGURANÇA DA INFORMAÇÃO ATRAVÉS DE CENTRO DE OPERAÇÃO DE SEGURANÇA 24X7

### 3.48.1. CARACTERÍSTICAS GERAIS

3.48.1.2. O monitoramento das soluções de segurança atualmente em produção no parque tecnológico do CONTRATANTE, se dará apenas para o serviço de segurança e não ficará a responsabilidade da CONTRATADA o fornecimento de licenças, suporte no produto, atualização de versão, correção de patches etc.

3.48.1.2. O monitoramento dos ativos de segurança do ambiente da CONTRATANTE deverá ser realizado através de ferramenta (hardware e/ou software) que coletará as informações necessárias via agente ou sem agente para o monitoramento de segurança (SOC).

3.48.1.4. Os serviços descritos neste termo de referência serão realizados totalmente baseados nas ferramentas de segurança que serão entregues nesta contratação.

3.48.1.5. As ferramentas que deverão ser entregues durante os serviços estão descritas com seus requisitos técnicos de atendimento para o ambiente da CONTRATANTE.

3.48.1.6. Todo o processo de serviços descritos neste edital será realizado conforme requisitos descritos das ferramentas de segurança da informação.

3.48.1.7. O acesso à solução de monitoramento deverá ser realizado apenas pela equipe de segurança da CONTRATANTE e pela equipe de serviço de SOC da CONTRATADA.

3.48.1.8. Deverão ser realizadas reuniões trimestrais gerenciais para avaliação e acompanhamento dos serviços contratados.

3.48.1.9. A CONTRATADA deverá monitorar alertas gerados pelas soluções de Segurança, envolvendo atividades como, por exemplo:

3.48.1.9.1. Alta disponibilidade;

3.48.1.9.2. Atividades de Rede;

3.48.1.9.3. Atividades de Ameaças;

3.48.1.9.4. Atividades do Túnel IPsec;

3.48.1.9.5. Falhas de interfaces dos equipamentos;

3.48.1.9.6. Consumo de link de internet;

3.48.1.9.7. Controle de Aplicações;

3.48.1.9.8. Atualizações de vacinas;

3.48.1.9.9. Endpoints em quarentena;

3.48.1.9.10. Lista de vulnerabilidades;

3.48.1.9.11. Monitoramento dos scanners de vulnerabilidade;

3.48.1.9.12. Vazamento de credenciais;

3.48.1.9.13. Comportamento anômalo.

3.48.1.10. A CONTRATADA poderá apoiar o processo de resposta a Incidentes de Segurança, com os relatórios extraídos da ferramenta e processos como varredura e análise de logs nas soluções de segurança da informação.

3.48.1.11. A CONTRATADA deverá produzir Relatório de Incidente de Segurança.

3.48.1.12. A CONTRATADA deverá produzir Boletins e indicadores de SI.

3.48.1.13. Entrega de relatório mensal com análise dos indicadores de comprometimento e anomalias detectadas e recomendações para melhoria dos modelos de correlação aplicados.

3.48.1.14. Apresentação de relatório mensal com análise de tendências de incidentes de segurança da informação.

3.48.1.15. A CONTRATADA deverá apoiar o processo de Resposta a Incidentes de Segurança.

3.48.1.16. Deverá avaliar situações em que o ambiente esteja sob ataque ou risco iminente de ataque, provendo o conhecimento e experiência necessários para as medidas de preparação, mitigação, contenção, defesa e resposta apropriadas quando possível executar os pontos listados.

3.48.1.17. CANAIS DE COMUNICAÇÃO Para abertura de solicitações, a CONTRATADA deverá disponibilizar 03 (três) tipos de canais de comunicação, a saber:

| Item | Descrição | Classificação |
|---|---|---|
| 1 | Linha de telefonia gratuita (0800.) | Tipo 1 |
| 2 | E-mail com domínio registrado e de propriedade da CONTRATADA. | Tipo 2 |
| 3 | Sistema de ITSM do inglês Information Technology Service Management (Gerenciamento de Serviços de TI). | Tipo 3 |

Tabela 1: TIPOS DE CANAIS DE COMUNICAÇÃO

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

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

3.48.1.20. Os SERVIÇOS GERENCIADOS DE SEGURANÇA, devem obrigatoriamente serem executados, ofertados, e estarem acessíveis ao ORGÃO CONTRATANTE em regime de 24 (vinte quatro) horas por dia, 07 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, durante todo o período de vigência do contrato.

## 3.49. MODALIDADE DE ATENDIMENTO

3.49.1. A modalidade principal de atendimento será remota, ou seja, realizada nas dependências da CONTRATADA, obedecendo obrigatoriamente aos critérios estabelecidos para sua execução, conforme previsto neste termo de referência.

3.49.2. Informações sobre o ambiente a ser suportado:

| Infraestrutura | | |
|---|---|---|
| Descrição | Tipo/Modelo | Quantidade |
| Estações de trabalho | Windows | 805 |
| Servidores físicos | Appliance | 5 |
| Servidores virtuais | VMware | 245 |
| Banco de dados | Oracle, MSSQL, PostgreSQL, Maria DB | 15 |
| Switches | Ruckus | 29 |
| Access Points | Extreme | 250 |
| Usuários de rede | Windows AD | 1259 |
| Usuários de VPN | Firewall | 1200 |

Tabela 2: INFORMACOES DO AMBIENTE CAMADA DE INFRAESTRUTURA

## 3.50. ACESSIBILIDADE E CONFIDENCIALIDADE

3.50.1. Para garantir a qualidade e disponibilidade dos serviços remotos, entre o ORGÃO CONTRATANTE e os 02 (dois) CSOC da CONTRATADA, deverá haver conexões digitais com ambos CSOC da CONTRATADA.

3.50.2. A fim de garantir a segurança do tráfego bidirecional entre o ORGÃO CONTRATANTE e os CSOC da C CONTRATADA, ambas as conexões devem ser criptografadas. Ou seja, a CONTRATADA deverá estabelecer duas VPN's (Virtual Private Network), do tipo site to site, para cada CSOC.

3.50.3. A fim de garantir a segurança entre o ORGÃO CONTRATANTE e os CSOC da CONTRATADA, não será permitido CSOC terceirizado ou consórcio de empresas. A CONTRATADA deve ter e manter um CSOC próprio.

3.50.4. A CONTRATADA deve assinar e entregar ao ORGÃO CONTRATANTE na reunião de alinhamento no início da vigência do contrato, termo de confidencialidade e sigilo, conforme modelo contido no Termo de Referência – Termo de Confidencialidade e Sigilo. Esse documento estabelece as condições para a prestação dos serviços acerca do sigilo das informações custodiadas, do acesso restrito das informações aos técnicos designados no

projeto, e da propriedade intelectual de todos os produtos e conhecimentos advindos da execução do contrato.

3.50.5. Além disso, o termo de confidencialidade e sigilo deve ser lido e assinado por todos os funcionários que venham executar os serviços, direta ou indiretamente, no âmbito do contrato, sendo que o ORGÃO CONTRATANTE pode solicitar, a qualquer momento, a comprovação desta obrigação. O respectivo termo deve ser entregue antes do início das atividades, mediante solicitação do ORGÃO CONTRATANTE.

3.50.6. Por outro lado, a CONTRATADA deve revogar todas as credenciais relacionadas a soluções de responsabilidade da CONTRATADA, empregadas na prestação de serviços ao ORGÃO CONTRATANTE, bem como solicitar a revogação destas ao ORGÃO CONTRATANTE, para soluções de responsabilidade da CONTRATADA, no mesmo dia do encerramento das atividades.

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

## 3.51. QUALIFICAÇÃO TÉCNICA DO SERVIÇO PRESTADO PELA CONTRATADA

3.51.1. Descrever a qualificação técnica da CONTRATADA é crucial para garantir a competência e a expertise necessárias para a execução eficaz do serviço contratado, assegurando a entrega de resultados de alta qualidade e a minimização de riscos operacionais.

## 3.52. ESTRUTURA PRÉ-EXISTENTE NA DATA DA LICITAÇÃO

3.52.1. Possuir estrutura central para visualização dos painéis dos sistemas de suporte técnico, monitoramento, administração e gerenciamento que permita que todos os profissionais visualizem eventos relevantes simultaneamente (BRASIL, NUVEM).

## 3.53. DISPONIBILIDADE

3.53.1. Para a prestação dos serviços remotos, o licitante que vier a ser contratado deverá utilizar-se de, pelo menos, 02 (dois) Centros de Operações de Segurança próprios, para garantir que a indisponibilidade de um deles não afete nenhum aspecto dos serviços prestados.

3.53.2. Estar conectado aos datacenters que hospedam os sistemas de suporte técnico, monitoramento, administração e gerenciamento através de múltiplas conexões de rede local, VPN ou WAN de forma que a falha de uma conexão isoladamente não afete o acesso aos mesmos.

## 3.54. LOCALIZAÇÃO

3.54.1. Os SOCs devem estar localizados no Brasil e já devem estar em pleno funcionamento na data da abertura da licitação.

## 3.55. REQUISITOS DE SEGURANÇA

3.55.1. A infraestrutura dos SOCs deve possuir mecanismos de segurança física e lógica necessários para garantir a segurança das informações, do ambiente operacional e alta disponibilidade. Cada um deles deve atender aos seguintes requisitos mínimos:

3.55.2. Efetue registro dos visitantes com identificação individual e controle digital de entrada e saída.

3.55.3. Possua Circuito Interno de TV para registro e gravação de imagem em todas as áreas de circulação.

3.55.4. Funcione em regime 24x7x365.

3.55.5. Todos os registros de segurança devem ser armazenados para consulta por ao menos 90 dias.

## 3.56. VISTORIAS

3.56.1. A CONTRATANTE poderá fazer vistoria para comprovar que as exigências contidas nesta especificação serão atendidas pela CONTRATADA.

## 3.57. DA EQUIPE

3.57.1. O quadro de profissionais do centro de operação de segurança SOC da contratada deverá atender às demandas previstas no contrato de acordo com a experiência e capacitações técnicas aqui indicadas, conforme item 2.1.30 Papéis.

## 3.58. COMPROVAÇÃO

3.58.1. Será exigido no momento da contratação as comprovações que se seguem:

3.58.2. A comprovação da experiência profissional, requerida para cada um dos perfis a seguir descritos, dar-se-á mediante a apresentação de documento emitido pela(s) empresa(s) onde o técnico realizou tarefas típicas da função pleiteada, exigindo-se similaridade com as tarefas relacionadas para cada perfil profissional.

3.58.3. A comprovação da capacitação técnica dar-se-á mediante a apresentação, para cada profissional, de original ou cópia autenticada dos certificados, conforme perfil exigido, dentro do período de validade.

3.58.4. Deverá ser comprovado o vínculo profissional do funcionário, CLT, fornecendo cópia da carteira de trabalho.

## 3.59. VERIFICAÇÕES

3.59.1. A CONTRATADA poderá solicitar entrevistas com quaisquer dos profissionais que participarão do projeto/serviços, objetivando análise técnica, em caso de dúvidas em relação ao atendimento de qualquer requisito documentado.

## 3.60. SUBSTITUIÇÕES

3.60.1. A CONTRATADA poderá solicitar, a qualquer tempo, a substituição de quaisquer dos profissionais envolvidos no projeto/serviços que apresentem desempenho insatisfatório na execução dos serviços contratados ou comportamento inadequado às regras de conduta vigentes na Instituição. Em qualquer caso, a CONTRATADA deverá substituir, mediante solicitação e a critério da CONTRATADA, qualquer profissional, sem ônus de qualquer natureza.

3.60.2. Caso ocorra o desligamento de qualquer um dos profissionais exigidos durante a vigência do contrato, a empresa deverá providenciar um substituto, com as mesmas qualificações, no prazo máximo de 15 dias.

## 3.61. PAPÉIS

3.61.1. Para a execução dos serviços, a CONTRATADA irá dispor de profissionais que executarão os serviços.

## 3.62. COORDENADOR / LÍDER TÉCNICO

| | |
|---|---|
| **Experiência Profissional** | • Comprovar vivência em segurança da informação de no mínimo 2 (dois) anos. |
| **Formação/Capacitação** | • Graduação em curso de TI;<br>• Pós-graduação em Segurança da Informação. |
| **Certificações Técnicas**<br>No mínimo 1 (um) dos Profissionais deverá ter no mínimo 5 (cinco) das certificações descritas | • Certified Information Security Manager (CISM).<br>• Certified Information Systems Security Professional<br>• (CISSP);<br>• EC-Council Certified Ethical Hacker Master.<br>• EC-Council Certified Ethical Hacker Practical.<br>• CompTIA Security +;<br>• CompTIA CySA+;<br>• CompTIA CASP+;<br>• CompTIA CSAP;<br>• CompTIA Linux+;<br>• EC-Council Certified SOC Analyst (CSA);<br>• EC-Council Certified Incident Handler (E\|CIH);<br>• GIAC Certified Incident Handler (GCIH);<br>• GIAC Continuous Monitoring Certification (GMON);<br>• EXIN ISFS Foundation;<br>• Linux Professional LPIC; |

| | |
|---|---|
| | • Vulnerability Management Foundation; |

## 3.63. EQUIPE TÉCNICA

| | |
|---|---|
| **Experiência Profissional** | • Comprovar vivência em segurança da informação.<br>• Comprovar experiência em instalação, customização, configuração e suporte técnico em segurança da informação. |
| **Formação/Capacitação** | • Graduação em curso de TI;<br>• Pós-graduação em Segurança da Informação. |
| **Certificações Técnicas**<br>A equipe deverá conter no mínimo 2 (dois) Profissionais com mínimo 2 (duas) das certificações descritas | • EC-Council Certified Ethical Hacker Master.<br>• EC-Council Certified Ethical Hacker Practical.<br>• EC-Council Certified Ethical Hacker.<br>• CompTIA Security +;<br>• CompTIA CySA+;<br>• CompTIA CSAP;<br>• EC-Council Certified SOC Analyst (CSA).<br>• EC-Council Certified Incident Handler (E\|CIH).<br>• GIAC Certified Incident Handler (GCIH).<br>• GIAC Continuous Monitoring Certification (GMON).<br>• EXIN ISFS Foundation;<br>• EXIN EHF;<br>• Linux Professional LPIC;<br>• Vulnerability Management Foundation; |

## 3.64. INTELIGÊNCIA DE AMEAÇAS

### 3.64.1. CARACTERÍSTICAS GERAIS DO SERVIÇO DE INTELIGÊNCIA DE AMEAÇAS

3.64.1.1. Deve possuir interface de gerenciamento no idioma Português do Brasil, Inglês e Espanhol;

3.64.1.2. Ter interface web via cloud pública;

3.64.1.3. Ser compatível com navegadores Mozilla Firefox, versão 60.0 ou superior, Google Chrome versão 65 ou superior;

3.64.1.4. O serviço deverá ser em nuvem de responsabilidade da CONTRATADA com acesso realizado via web no modelo SaaS (Software-as-a-Service);

3.64.1.5. Uma vez que os eventos forem coletados pela ferramenta, estes devem permanecer disponíveis por tempo indeterminado, mesmo que haja remoção original do conteúdo;

3.64.1.6. Deverá garantir acesso simultâneo para 05 (cinco) usuários;

3.64.1.7. Permitir integração com API REST com suporte no retorno de informações no padrão JSON;

3.64.1.8. Permitir a integração a ferramentas externas por meio de API REST e/ou SDK;

3.64.1.9. Deve possuir API com controle de acesso baseado em usuário e times para consumo de informações via outras ferramentas;

3.64.1.10. Deve possibilitar integração com MISP;

3.64.1.11. A plataforma deve ter mecanismo de armazenamento de logs de acesso dos usuários por um período mínimo de 1 ano;

3.64.1.12. A solução deverá possuir, pelo menos, 6 bilhões de eventos coletados e indexados;

3.64.1.13. A solução deverá possuir, pelo menos, 20 (vinte) milhões de atores maliciosos monitorados;

3.64.1.14. Os logs de acesso devem ser armazenados com no mínimo as seguintes informações:

3.64.1.14.1. Usuário;

3.64.1.14.2. Atividade executada;

3.64.1.14.3. IP de acesso;

3.64.1.14.4. Data e hora de acesso;

3.64.1.14.5. User Agent;

3.64.1.15. A plataforma deve disponibilizar manual do usuário;

3.64.1.16. Possuir análise de dados coletados, fornecendo um painel de visualização que contemple, no mínimo, as seguintes funcionalidades:

3.64.1.16.1. Visualização de perfis relacionados a palavras-chaves;

3.64.1.16.2. Realização de buscas nos dados incluindo buscas avançadas com critérios e entidades diferentes;

3.64.1.16.3. Permitir a navegação com clicks nos tipos de informações de interesse do painel, com apresentação das informações relacionadas.

3.64.1.16.4. Apresentação dos dados buscados em painéis com as principais fontes identificadas na busca;

3.64.1.16.5. Exportar as informações identificadas em relatórios via XLSX, JSON, CSV, DOCX e PDF.

3.64.1.17. Deve realizar etapa de pós-processamento nos eventos coletados:

3.64.1.17.1. Realização de OCR (Optical Character Recognition) nas imagens indexadas pela plataforma;

3.64.1.17.2. Transcrição dos áudios e vídeos indexados na plataforma;

3.64.1.17.3. Detecção automática de linguagem;

3.64.1.17.4. Extração de metadados relevantes dos eventos para cada fonte passível de coleta;

3.64.1.17.5. Deve realizar detecção automática, com uso de Inteligência Artificial de, pelo menos:

3.64.1.17.5.1. Cartões de crédito vazados;

3.64.1.17.5.2. Credenciais vazadas;

3.64.1.18. Os metadados coletados em cada evento devem incluir no mínimo:

3.64.1.18.1. Data original do evento;

3.64.1.18.2. Hash do conteúdo que permite a desduplicação de informações disponíveis;

3.64.1.18.3. Data de indexação do evento;

3.64.1.18.4. Fonte original da informação;

3.64.1.18.5. Robô responsável pela coleta da informação;

3.64.1.18.6. Informações pertinentes da fonte que originou o evento;

3.64.1.19. Disponibilizar mecanismo para busca das informações permitindo:

3.64.1.19.1. Busca por intervalo de data;

3.64.1.19.2. Busca por metadados específicos;

3.64.1.19.3. Busca por fontes de informação;

3.64.1.19.4. Busca por palavras-chaves;

3.64.1.20. Disponibilizar através de interface web, a busca utilizando mecanismos como:

3.64.1.20.1. Proximidade;

3.64.1.20.2. Fuzzy (difusa);

3.64.1.20.3. Lógica binária;

3.64.1.20.4. Expressões regulares (regex);

3.64.1.20.5. Operadores lógicos (“AND, “OR” e “NOT”);

3.64.1.20.6. Caracteres wildcard;

3.64.1.21. Permitir a ordenação dos resultados por data da postagem mais recente para a mais antiga;

3.64.1.22. Permitir a escolha da quantidade de resultados por página;

3.64.1.23. Permitir salvar o resultado da pesquisa;

3.64.1.24. Deve possuir mecanismo que permita que buscas criadas possam ser salvas para uso posterior;

3.64.1.25. Deve permitir a identificação de links patrocinados;

3.64.1.26. Deve permitir a identificação de perfis falsos;

3.64.1.27. Deve permitir a identificação de campanhas e ataques “zero-day”;

3.64.1.28. Deve permitir a identificação de campanhas de phishing;

3.64.1.29. Deve permitir a identificação de defacement de páginas;

3.64.1.30. Deve permitir a identificação da comercialização ilegal de vulnerabilidades ou ativos de interesse da CONTRATANTE;

3.64.1.31. Deve permitir o acompanhamento de discussões de assuntos que coloquem em risco os ativos, pessoas ou serviços de interesse da CONTRATANTE;

3.64.1.32. Deve identificar a emissão de certificados de domínios monitorados;

3.64.1.33. Deve identificar a criação de domínios de recursos monitorados;

3.64.1.34. Deve realizar consulta Whois de forma automática nos Bots que realizam coletas de domínios;

3.64.1.35. Deve processar URLs de maneira automática para a detecção de phishings aplicando técnicas de machine-learning;

3.64.1.36. Deve guardar preview dos sites de phishing;

3.64.1.37. Deve fazer o download automático do código fonte de sites detectados como phishing;

3.64.1.38. A ferramenta deve permitir o drill-down das pesquisas utilizando filtros inclusivos e exclusivos;

3.64.1.39. Possuir um dashboard para análise dos dados coletados com no mínimo as seguintes informações:

3.64.1.39.1. Gráfico com a quantidade de informações de acordo com as palavras ou termos buscados;

3.64.1.39.2. Divisão dos dados por tipo de dado encontrado (imagem, texto, áudio, etc);

3.64.1.39.3. Principais perfis;

3.64.1.39.4. Principais fontes de dados;

3.64.1.39.5. Principais grupos;

3.64.1.40. Permitir a busca de perfis específicos, usando nome/apelido, número de telefone ou e-mail, com no mínimo os seguintes campos:

3.64.1.40.1. Fonte;

3.64.1.40.2. Nome;

3.64.1.40.3. Apelido;

3.64.1.40.4. Telefone;

3.64.1.40.5. Grupos.

3.64.1.41. Possuir um painel de visualização de todas as pesquisas salvas, possibilitando a execução dessas pesquisas salvas.

3.64.1.42. Permitir a pesquisa por uma busca salva específica.

3.64.1.43. Permitir filtrar as buscas salvas por empresa.

3.64.1.44. Permitir a edição e atualização de uma busca salva.

3.64.1.45. Deve permitir a criação/alteração/exclusão de variáveis na plataforma, possibilitando gerenciamento de termos ou buscas dentro dessa variável.

3.64.1.46. Deve permitir a notificação de eventos relevantes em forma de ocorrências para outros usuários em times dentro da organização.

3.64.1.47. Deve permitir a associação de múltiplos eventos a uma mesma ocorrência.

3.64.1.48. Deve ser possível visualizar diretamente nos eventos a(s) ocorrência(s) em que o dado evento foi associado.

3.64.1.49. As ocorrências devem possuir um campo de descrição em que os analistas possam contextualizar as informações associadas.

3.64.1.50. O campo de descrição das ocorrências deve permitir a cópia e colagem de imagens de forma que possam ser vistas in-line.

3.64.1.51. As ocorrências devem permitir o upload de arquivos como anexo.

3.64.1.52. Deve ser possível notificar via e-mail e via WebHook a criação e modificação de ocorrências aos times envolvidos.

3.64.1.53. Deve permitir a criação de títulos para fácil identificação das ocorrências.

3.64.1.54. Deve possuir um painel de gerenciamento das ocorrências, possibilitando a busca com as seguintes opções:

3.64.1.54.1. Busca por palavras-chave;

3.64.1.54.2. Busca por número da ocorrência;

3.64.1.54.3. Deve ser possível buscar nos metadados dos eventos dentro das ocorrências.

3.64.1.55. Possuir um filtro para busca de ocorrências com no mínimo as seguintes opções:

3.64.1.55.1. Categoria;

3.64.1.55.2. Status;

3.64.1.55.3. Período;

3.64.1.55.4. Responsável pela criação;

3.64.1.55.5. Time responsável.

3.64.1.56. No painel de gerenciamento, deve ser possível visualizar a quantidade total de ocorrências e ordenar por data e prioridade.

3.64.1.57. Permitir a adição de IOCs dentro das ocorrências.

3.64.1.58. Permitir visualizar um histórico com log de alterações das ocorrências.

3.64.1.59. Deve permitir a classificação das ocorrências através de categorias.

3.64.1.60. Deve permitir a classificação das ocorrências de acordo com a criticidade.

3.64.1.61. Deve permitir a definição de times responsáveis por cada ocorrência.

3.64.1.62. Deve permitir a adição de comentários ilimitados a cada ocorrência.

3.64.1.63. Deve permitir filtrar por organização e empresas.

3.64.1.64. Deve fazer detecção e extração de cartões de crédito e débito expostos nos eventos da plataforma.

3.64.1.65. Deve possuir, (se necessário) a capacidade de ter no mínimo, 12 (doze) milhões de cartões de crédito e débito expostos coletados e indexados na plataforma.

3.64.1.66. Deve possuir um dashboard para apresentação de informações sobre cartões expostos, contendo:

3.64.1.66.1. Quantidade de cartões expostos por período;

3.64.1.66.2. Bandeiras;

3.64.1.66.3. Categorias;

3.64.1.66.4. Emissores;

3.64.1.66.5. Países.

3.64.1.67. Possibilidade de filtrar por períodos e empresas.

3.64.1.68. Possibilidade de visualizar a quantidade de cartões expostos encontrados na busca.

3.64.1.69. Deve permitir filtrar por organização e empresas.

3.64.1.70. Além dos eventos, a ferramenta deve contar com relatórios periódicos, desenvolvidos pelo time de inteligência do fabricante, com informações, ameaças, botnets, tendências, campanhas de hacktivismo em andamento, perfis de atores maliciosos, indicadores de comprometimento e avisos informativos gerais.

3.64.1.71. Os relatórios devem ser gerados sempre que identificado um assunto pertinente relacionado aos temas acima e deve possuir ao menos 7 relatórios publicados por semana.

3.64.1.72. Deve permitir a busca desses relatórios por palavras-chave.

3.64.1.73. Deve permitir visualizar a quantidade de relatórios encontrados na busca.

3.64.1.74. Deve possuir um mínimo de 2 mil relatórios na base de dados.

3.64.1.75. Os relatórios devem estar disponíveis, no mínimo, nos seguintes idiomas: português, inglês e espanhol.

3.64.1.76. Deve permitir filtrar a busca de relatórios por, no mínimo:

3.64.1.76.1. Categorias;

3.64.1.76.2. Período.

3.64.1.77. Deve apresentar informações pertinentes de acordo com cada assunto, como IOCs, anexos e IPs que possam ser interessantes ao cliente.

3.64.1.78. Deve permitir o download desse relatório no mínimo em formato PDF.

3.64.1.78.1. Para relatórios com classificação confidencial, este deverá ser cifrado com senha individual, com o objetivo de evitar compartilhamento acidental de informações sensíveis.

3.64.1.79. O sistema deverá possuir mecanismo de captura automatizado de informações em diversas fontes da internet, incluindo, no mínimo:

3.64.1.79. O sistema deverá possuir mecanismo de captura automatizado de informações em diversas fontes da internet, incluindo, no mínimo:Mídias sociais:

3.64.1.80.1. Facebook.

3.64.1.80.2. Facebook ADS.

3.64.1.80.3. Twitter.

3.64.1.80.4. LinkedIn.

3.64.1.80.5. Instagram.

3.64.1.80.6. TikTok.

3.64.1.80.7. YouTube.

3.64.1.80.8. Koo App.

3.64.1.80.9. Mastodon;

3.64.1.80.10. Pinterest;

3.64.1.80.11. Volo;

3.64.1.80.12. Twitch.

3.64.1.81. Aplicações de mensageria instantâneas:

3.64.1.81.1. WhatsApp.

3.64.1.81.2. Telegram.

3.64.1.81.3. IRC.

3.64.1.81.4. Discord.

3.64.1.81.5. Slack.

3.64.1.82. Motores de busca:

3.64.1.82.1. Google;

3.64.1.82.2. Yahoo;

3.64.1.82.3. Bing;

3.64.1.82.4. DuckDuckGo.

3.64.1.83. Sites de e-commerce:

3.64.1.83.1. OLX;

3.64.1.83.2. Mercado Livre.

3.64.1.84. Lojas de aplicativos oficiais e não-oficiais:

3.64.1.84.1. Aptoide.

3.64.1.84.2. Google Play/apkpure.

3.64.1.85. Chans:

3.64.1.85.1. 4Chan.

3.64.1.85.2. Kohlchan.

3.64.1.85.3. Leftypol.

3.64.1.85.4. Vhs Chan.

3.64.1.85.5. Vecchiochan.

3.64.1.85.6. Mlpol.Net.

3.64.1.85.7. Chan.

3.64.1.85.8. Sportschan.

3.64.1.85.9. 8Kunchan.

3.64.1.85.10. Endchan.

3.64.1.85.11. 27Chan.

3.64.1.85.12. Tvchan.

3.64.1.85.13. Lainchan.

3.64.1.85.14. Wired-7.

3.64.1.85.15. Leftychan.

3.64.1.85.16. Niuchan.

3.64.1.85.17. Erischan.

3.64.1.85.18. Anonima Club.

3.64.1.85.19. 75Chan.

3.64.1.85.20. 8Chan.

3.64.1.85.21. Intern3Ts.

3.64.1.85.22. 1Chan.Us.

3.64.1.85.23. 83channel.

3.64.1.86. Fóruns de discussão:

3.64.1.86.1. Hack Forums;

3.64.1.86.2. Patched.

3.64.1.86.3. Club2Crd.

3.64.1.86.4. Carder UK.

3.64.1.86.5. Bleeping Computer.

3.64.1.86.6. Guia Do Hacker;

3.64.1.86.7. Leak Base;

3.64.1.86.8. Xss Is.

3.64.1.86.9. Sinister.

3.64.1.86.10. Leaks.

3.64.1.86.11. Partner IT.

3.64.1.86.12. Sinful.

3.64.1.86.13. Exploitin.

3.64.1.86.14. Cryptbb.

3.64.1.86.15. Verified Carder.

3.64.1.86.16. Perfect Hackers.

3.64.1.86.17. Blackbones.

3.64.1.86.18. Shield.

3.64.1.86.19. Leakforums;

3.64.1.86.20. Ramp;

3.64.1.86.21. Altenen;

3.64.1.86.22. Forum 1877.

3.64.1.87. Repositórios de códigos:

3.64.1.87.1. GitHub.

3.64.1.87.2. Bitbucket.

3.64.1.87.3. GitLab.

3.64.1.88. Indexadores de malware:

3.64.1.88.1. Anyrun.

3.64.1.88.2. Hybrid Analysis.

3.64.1.88.3. Malware Bazaar.

3.64.1.88.4. Ransomware;

3.64.1.88.5. VirusTotal.

3.64.1.89. Serviços de paste:

3.64.1.89.1. Pastebin;

3.64.1.89.2. Ghostbin.

3.64.1.90. Feed de domínios:

3.64.1.90.1. CertStream.

3.64.1.90.2. Open Phish;

3.64.1.90.3. Phishtank;

3.64.1.90.4. Whoxy;

3.64.1.90.5. Zone Files IO.

3.64.1.90.6. Fuzzydns;

3.64.1.90.7. URL Scan.

3.64.1.90.8. URL Haus.

3.64.1.91. Vulnerabilidades:

3.64.1.91.1. CVE;

3.64.1.91.2. Circl.lu;

3.64.1.91.3. Open Bug Bounty;

3.64.1.91.4. ExploitDB.

3.64.1.92. Serviços/Dispositivos de rede:

3.64.1.92.1. Binary Edge;

3.64.1.92.2. Censys;

3.64.1.92.3. Shodan;

3.64.1.92.4. Zoom Eye;

3.64.1.92.5. LeakIX.

3.64.1.93. Defacement:

3.64.1.93.1. MirrorH;

3.64.1.93.2. Zone-H.

3.64.1.94. Blogs de grupos de ransomware:

3.64.1.94.1. Blackcat (Alphvm);

3.64.1.94.2. Medusa;

3.64.1.94.3. Clop;

3.64.1.94.4. Lockbit;

3.64.1.94.5. Black Basta;

3.64.1.94.6. Blackbyte Auction;

3.64.1.94.7. Play;

3.64.1.94.8. Unsafe;

3.64.1.94.9. Bianlian;

3.64.1.94.10. Royal Landing;

3.64.1.94.11. Dunghill Leak;

3.64.1.94.12. Ragnar Locker;

3.64.1.94.13. Trigona;

3.64.1.94.14. Everest;

3.64.1.94.15. Money Message;

3.64.1.94.16. Karakurt;

3.64.1.94.17. Snatch;

3.64.1.94.18. Stormous;

3.64.1.94.19. Lorenz;

3.64.1.94.20. Vice Society;

3.64.1.94.21. Ransom House;

3.64.1.94.22. Abyss;

3.64.1.94.23. Crosslock;

3.64.1.94.24. Cryptnet;

3.64.1.94.25. Cuba;

3.64.1.94.26. Dark Leak.

3.64.1.94.27. External Threats;

3.64.1.94.28888. Grayhatwarfare;

3.64.1.94.29. ONION;

3.64.1.94.30. RSS;

3.64.1.94.31. The Pirate Bay;

3.64.1.95. A ferramenta deve permitir o direcionamento das coletas realizadas pela plataforma por meio da configuração de robôs de coleta.

3.64.1.96. Quanto à configuração dos robôs, deverá ser realizada através da interface web, sem a necessidade de codificação, da seguinte forma:

3.64.1.96.1. Deve permitir a configuração de mais de um robô por fonte;

3.64.1.96.2. Deve permitir a configuração do intervalo de execução e coleta de cada robô de forma individual;

3.64.1.96.3. Deve permitir a configuração da visibilidade das informações coletadas por cada robô para times específicos da organização;

3.64.1.96.4. Deve permitir a aplicação de filtros na coleta para direcionamento das informações que entram na plataforma.

3.64.1.97. A ferramenta deve permitir a configuração de Google-Dorks para buscas direcionadas ao Google.

3.64.1.98. Em relação ao monitoramento de grupos de Ransomware:

3.64.1.98.1. A solução deverá monitorar e possuir em sua base, pelo menos, 30 mil eventos de ransomware.

3.64.1.99. A ferramenta deve possuir um dashboard para apresentação de informações sobre eventos e grupos de ransomware, contendo:

3.64.1.99.1. Eventos com as postagens dos blogs monitorados;

3.64.1.99.2. Principais grupos com mais postagens nos blogs monitorados;

3.64.1.99.3. Gráfico com a quantidade de eventos publicados por dia;

3.64.1.99.4. Relatórios relacionados aos ransomwares.

3.64.1.100. A ferramenta deve mapear os principais grupos de Ransomware detectados.

3.64.1.101. A ferramenta deve possuir mecanismo de múltiplo fator de autenticação (MFA).

3.64.1.102. A ferramenta deverá possuir suporte à Single Sign-on (SSO):

3.64.1.102.1. Azure;

3.64.1.102.2. OKTA.

3.64.1.103. A ferramenta deve permitir, no mínimo, configurar, habilitar e desabilitar múltiplos logins de usuários, complexidade de senhas, troca de senha no primeiro login, troca de senha periodicamente, ativação e desativação de usuários, definição de grupos e times.

3.64.1.104. A ferramenta deve disponibilizar usuários com perfil de administrador para acesso aos recursos da ferramenta, bem como acesso aos dados e alertas de outros usuários.

3.64.1.105. A ferramenta deve permitir que, dentro de uma mesma organização, seja possível a criação de empresas distintas, onde seja possível indicar os times com acesso às informações desta empresa.

3.64.1.106. Quanto ao permissionamento de usuários:

3.64.1.106.1. Deverá ser possível dar permissões e papéis diferenciados para os usuários configurados na plataforma.

3.64.1.107. A ferramenta deve permitir salvar consultas para disponibilizar para outros usuários.

3.64.1.108. A ferramenta deve permitir criar, gerenciar e excluir alertas.

3.64.1.109. A ferramenta deve permitir salvar tabelas de dicionários para o uso em pesquisas.

3.64.1.110. A ferramenta deve permitir a configuração de empresas com, no mínimo, os seguintes atributos:

3.64.1.110.1. Times de acesso;

3.64.1.110.2. Palavras-chave;

3.64.1.110.3. Ranges de IP;

3.64.1.110.4. Domínios;

3.64.1.110.5. ASNs;

3.64.1.110.6. Websites;

3.64.1.110.7. White-lists;

3.64.1.110.8. Palavras-chave VIPs.

3.64.1.111. A ferramenta deve possuir perfil de administrador e usuário normal dentro da organização.

3.64.1.112. Deve ser possível criar novas categorias de perfil com granularidade de acesso por funcionalidade da plataforma (RBAC).

3.64.1.113. A ferramenta deve permitir a configuração de alertas diretamente via interface de gerenciamento.

3.64.1.114. A ferramenta deve permitir realizar testes de funcionamento dos alertas configurados via interface de gerenciamento.

3.64.1.115. A ferramenta deve permitir a configuração de alertas via E-mail, Webhook, SMS, Ocorrências/Tickets e WhatsApp.

3.64.1.116. A ferramenta deve permitir a configuração de alertas baseados em:

3.64.1.116.1. Consultas/pesquisas salvas;

3.64.1.116.2. CPF vazado/exposto;

3.64.1.116.3. Citações de pessoas importantes (VIP);

3.64.1.116.4. Credenciais de domínios cadastrados.

3.64.1.117. A ferramenta deve permitir consultar credenciais de usuários expostas na internet:

3.64.1.117.1. Credenciais expostas em bases externas;

3.64.1.117.2. Credenciais expostas por malware;

3.64.1.117.3. Credenciais detectadas nos eventos da plataforma.

3.64.1.118. A ferramenta deve possuir um dashboard com informações gerais sobre as credenciais da organização que foram vazadas.

3.64.1.119. A ferramenta deve possuir uma tela de pesquisa onde seja possível efetuar a busca por credenciais baseados em domínios, subdomínios, e-mails específicos e URLs de acesso.

3.64.1.120. A ferramenta deverá possuir, no mínimo, 7 bilhões de credenciais expostas na base de dados.

3.64.1.121. A ferramenta deve permitir filtrar os resultados da busca por data de recebimento da credencial vazada e por tipo de vazamento.

3.64.1.122. A ferramenta deve permitir a busca de credenciais utilizando mecanismos como:

3.64.1.122.1. Proximidade;

3.64.1.122.2. Fuzzy (difusa);

3.64.1.122.3. Lógica binária;

3.64.1.122.4. Expressões regulares (regex);

3.64.1.122.5. Operadores lógicos (“AND, “OR” e “NOT”);

3.64.1.122.6. Caracteres wildcard.

3.64.1.123. A ferramenta deve possuir um dashboard com informações gerais sobre vulnerabilidades.

3.64.1.124. A ferramenta deve possuir informações gráficas sobre as principais CVEs identificadas.

3.64.1.125. A ferramenta deve apresentar relatórios relacionados às vulnerabilidades.

3.64.1.126. A ferramenta deve apresentar os últimos eventos detectados pela plataforma em relação às vulnerabilidades.

3.64.1.127. A ferramenta deve possuir uma interface que permita a pesquisa por vulnerabilidades por, no mínimo:

3.64.1.127.1. Busca textual;

3.64.1.127.2. Severidade;

3.64.1.127.3. Data.

3.64.2. Serviço de Takedown – Remoção de Conteúdo Malicioso

3.64.2.1.1. O serviço de inteligência de ameaças deverá contar com a funcionalidade de takedown.

3.64.2.1.2. Deve possuir uma tela para solicitação de takedowns, com no mínimo as seguintes opções:

3.64.2.1.3. URL para takedown;

3.64.2.1.4. Empresa;

3.64.2.1.5. Prioridade;

3.64.2.1.6. Categoria.

3.64.2.1.7. Deve ser possível adicionar um feedback às ocorrências fechadas, classificando o nível de relevância.

3.64.2.1.8. Deve possuir uma tela para visualização dos takedowns solicitados.

3.64.2.1.9. No painel de gerenciamento, deve ser possível visualizar a quantidade total de takedowns e ordenar por data e prioridade.

3.64.2.1.10. Deve possuir filtros para a busca de takedowns solicitados com no mínimo as seguintes opções de filtro:

3.64.2.1.10.1. Empresa;

3.64.2.1.10.2. Status;

3.64.2.1.10.3. Categoria;

3.64.2.1.10.4. Período;

3.64.2.1.10.5. Responsável pela criação;

3.64.2.1.10.6. Número da ocorrência;

3.64.2.1.10.7. Responsável pelo takedown.

3.64.2.1.11. Quanto ao takedown, a plataforma deve disponibilizar um dashboard com, pelo menos:

3.64.2.1.11.1. Quantidade de takedowns solicitados no período;

3.64.2.1.11.2. Status dos takedowns solicitados;

3.64.2.1.11.3. Tempo médio de mudança de status do takedown;

3.64.2.1.11.4. Lista de takedowns solicitados;

3.64.2.1.11.5. Aba de pesquisa de takedowns com filtro por ao menos:

3.64.2.1.11.6. Status;

3.64.2.1.11.7. Categoria;

3.64.2.1.11.8. Período.

## 3.65. SERVIÇO DE PROTEÇÃO DE PERÍMETRO

### 3.65.1. CARACTERÍSTICAS DO HARDWARE

3.65.1.1. Deve ser ofertado 1 equipamento.

3.65.1.2. Deve possuir throughput de, no mínimo, 2,6 (dois ponto seis) de Gbps de Next Generation Firewall considerando no mínimo as funcionalidades de Firewall e Controle de Aplicação, sendo comprovado com documentação de domínio público.

3.65.1.3. Deve possuir throughput de, no mínimo, 1,1 (um ponto um) Gbps com as funcionalidades de controle de aplicação, IPS, Antivírus, Anti-Spyware, Sandbox e log habilitadas simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os throughput aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real.

3.65.1.4. Deve suportar, no mínimo, 200.000 (duzentos mil) sessões simultâneas.

3.65.1.5. Deve suportar, no mínimo, 34.000 (trinta e quatro mil) novas sessões por segundo.

3.65.1.6. Deve possuir, no mínimo, 8 (oito) interfaces físicas de rede de 1 Gbps do tipo RJ-45.

3.65.1.7. Deve ser entregue com redundância em HA ativa-passiva.

3.65.1.8. Deve ter fonte redundante.

3.65.1.9. Deve ser entregue com trilho para instalação em rack de servidores, tamanho padrão.

3.65.1.10. Caso não exista trilho, deve ser entregue bandeja ou solução similar.

3.65.1.11. Deve possuir porta de gerência out-of-band 10/100/1000 RJ45.

3.65.1.12. Deve permitir até 2 (dois) sistemas virtuais sendo que deve vir 1 (um) já licenciado.

### 3.66. FUNCIONALIDADES GERAIS

3.66.1. A solução deve consistir em appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW) e console de gerência e monitoração.

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

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

3.66.4. A solução de segurança deve possuir nativamente funcionalidade de Machine Learning capaz de bloquear grande volume dos ataques nas suas redes.

3.66.5. Os Firewalls de segurança físico ou virtualizados devem possuir mecanismo para dedicar processamento no equipamento de segurança para funções e ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU, evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problemas. Entre as funções, deve suportar no mínimo: acesso SSH, acesso WEB, alterações de política, comunicação SNMP.

3.66.6. O hardware e software que executem as funcionalidades de proteção de rede devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistemas operacionais de uso genérico.

3.66.7. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

3.66.8. Agregação de links 802.3ad e LACP para o equipamento do tipo I.

3.66.9. Policy based routing ou policy based forwarding.

3.66.10. Roteamento multicast (PIM-SM).

3.66.11. DHCP Relay.

3.66.12. DHCP Server.

3.66.13. Jumbo Frames.

3.66.14. Suporte à criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3.

3.66.15. Suportar sub-interfaces ethernet lógicas.

3.66.16. Deve suportar os seguintes tipos de NAT:

3.66.17. NAT dinâmico (Many-to-1).

3.66.18. NAT dinâmico (Many-to-Many).

3.66.19. NAT estático (1-to-1).

3.66.20. NAT estático (Many-to-Many).

3.66.21. NAT estático bidirecional 1-to-1.

3.66.22. Tradução de porta (PAT).

3.66.23. NAT de Origem.

3.66.24. NAT de Destino.

3.66.25. Suportar NAT de Origem e NAT de Destino simultaneamente.

3.66.26. Deve implementar Network Prefix Translation (NPTv6).

3.66.27. Enviar log para sistemas de monitoração externos.

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

3.66.29. Deve permitir configurar certificado, caso necessário, para autenticação no sistema de monitoração externo de logs.

3.66.30. Proteção contra anti-spoofing.

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

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

3.66.33. Suportar a OSPF graceful restart.

3.66.34. Deve suportar o protocolo MP-BGP (Multiprotocol BGP), permitindo que o firewall possa anunciar rotas multicast para IPv4 e rotas unicast para IPv6.

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

3.66.36. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede. 3.66.37. Modo Camada 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação.

3.66.38. Modo Camada 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação, operando como default gateway das redes protegidas.

3.66.39. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.

3.66.40. Suporte à configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:

3.66.41. Em modo transparente.

3.66.42. Em Layer 3.

3.66.43. A configuração em alta disponibilidade deve sincronizar:

3.66.44. Sessões.

3.66.45. Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QoS e objetos de rede.

3.66.46. Certificados de-criptografados.

3.66.47. Associações de Segurança das VPNs.

3.66.48. Tabelas FIB.

3.66.49. No modo HA (modo de Alta Disponibilidade), deve possibilitar monitoração de falha de link.

3.66.50. Deve ser capaz de utilizar Machine Learning para realizar a descoberta de dispositivos IoT na rede com, pelo menos, 50 características, tais como: fabricante, tipo, versão de SO, etc.

3.66.51. Deve ser capaz de analisar o comportamento de dispositivos IoT com base em CVEs conhecidas.

3.66.52. A ferramenta deve possuir console centralizada, apresentando graficamente o inventário de todos os dispositivos detectados pela ferramenta.

3.66.53. Deve ser capaz de realizar avaliação de segurança nos dispositivos descobertos e sua classificação de riscos de segurança.
3.66.54. A solução deve ser capaz de apresentar opção de regra baseada em boas práticas de segurança.

3.66.55. Deve ser possível aplicar regras de segurança limitando o acesso do dispositivo (asset) identificado com outros dispositivos de rede.

3.66.56. Aplicar inspeção através de funcionalidades de segurança e bloqueio de tráfego dos dispositivos (assets) identificados para conter qualquer acesso indevido ou ameaça baseada em portas/serviços não autorizados.

3.66.57. Caso a solução não possua essas funcionalidades, será permitido a integração com ferramentas que executam esta função para, pelo menos, 15 mil dispositivos.

## 3.67. SD-WAN

3.67.1. Deve operacionalizar, no mínimo, os seguintes critérios de SD-WAN.

3.67.2. A plataforma de segurança deverá recuperar pacotes perdidos antes que seja necessário alterar o caminho principal.

3.67.3. As configurações de perfis de SD-WAN devem partir de um ponto central, permitindo alteração e criação dos elementos primordiais para o funcionamento da solução. Deve também entregar a criação automática dos túneis IPSEC entre as localidades.

3.67.4. A solução deve permitir operar em caráter de diagrama hub-spoke.

3.67.5. É considerado diferencial dispositivos que tenham a capacidade de exibir impactos por aplicação.

3.67.6. A solução deve permitir ao administrador métricas de utilização de banda por circuito disponível e, desta forma, exibir no mínimo os seguintes itens em porcentagem ou contadores: jitter, latência e perda de pacote.

3.67.7. O dispositivo deve compreender o que está causando desempenho de degradação para as aplicações e serviços ativos, garantindo que a experiência do usuário sofra o menor impacto possível.

3.67.8. O SD-WAN deve suportar os seguintes tipos de conexões WAN: ADSL/DSL, Cable Modem com Ethernet ou fibra, LT /3G/4G/5G, MPLS, Link de rádio e Link satélite, desde que a sua terminação permita conectividade com interfaces Ethernet.

3.67.9. A solução deve ter inteligência para executar, no mínimo, as seguintes lógicas de operação:

3.67.10. Distribuição de tráfego por prioridade de circuito; circuitos exclusivos de contingenciamento em 3G/4G/5G devem ser utilizados apenas em caso de falha geral dos circuitos ADSL/MPLS.

3.67.11. Distribuição de tráfego de acordo com métricas definidas por origem e destino. O dispositivo deve permitir ao administrador criar perfis com base em latência, jitter ou perda de pacotes.

3.67.12. Distribuição de tráfego com balanceamento de sessão entre os circuitos existentes.

3.67.13. Quando ambos os pontos de extremidade dos túneis SD-WAN estiverem ativos, deve haver a duplicação de pacotes (PD) para manter a experiência dos usuários, mesmo em condição de perda de pacotes. A duplicação de pacotes deve criar uma cópia do fluxo de tráfego do aplicativo e enviá-la em ambos os túneis disponíveis, que estão orientados ao mesmo destino.

3.67.14. O dispositivo de SD-WAN deve utilizar "Forward Error Correction" (FEC) habilitado para permitir que aplicativos sensíveis à perda de pacotes não sejam impactados em caso de perda de pacote e recupere os pacotes perdidos ou corrompidos usando pacotes de paridade incorporados no fluxo da comunicação. O objetivo é reparar o fluxo antes que ele precise fazer failover para outro caminho.

3.67.15. O SD-WAN deve permitir combinar vários serviços ISP em uma interface Ethernet Agregada (AE) para redundância de link. A interface agregada deve oferecer suporte a subinterfaces para que seja possível marcar diferentes serviços ISP usando tags de VLAN de camada 3 a fim de obter segmentação de tráfego de ponta a ponta.

3.67.16. O SD-WAN deve permitir o monitoramento de integridade do caminho de aplicativos SaaS para garantir decisões com base em confiabilidade e experiência do usuário. Nos

cenários onde o SD-WAN possui link de acesso direto à Internet (DIA), deve permitir o failover para um caminho de desempenho mais alto com base em medições precisas da qualidade da aplicação.

3.67.17. Distribuição orientada à qualidade: o dispositivo deve validar o melhor caminho disponível e utilizar esse "path" para manter sessões ativas. Caso o melhor caminho entre em degradação por fatores anômalos, o dispositivo deverá entender esses fatores e distribuir para os demais circuitos existentes.

## 3.68. CONTROLE POR POLÍTICA DE FIREWALL

3.68.1. Deverá suportar controles por zona de segurança.

3.68.2. Controles de políticas por porta e protocolo.

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

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

3.68.5. Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs, podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego.

3.68.6. Deve permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs.

3.68.7. Deve permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio firewall.

3.68.8. Controle de políticas por código de país (por exemplo: BR, USA, UK, RUS).

3.68.9. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e saída (Outbound).

3.68.10. Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound).

3.68.11. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com HTTP/2, TLS 1.2 e TLS 1.3.

3.68.12. Controle de inspeção e de-criptografia de SSH por política.

3.68.13. A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança.

3.68.14. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg.

3.68.15. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo).

3.68.16. QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações.

3.68.17. Suporte a objetos e regras IPv6.

3.68.18. Suporte a objetos e regras multicast.

3.68.19. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

3.68.20. Deve possuir ferramenta que indique as regras sobrepostas e objetos não utilizados para otimização das regras. Caso não possua essa funcionalidade, será permitido a integração com ferramentas que executam esta função.

## 3.69. CONTROLE DE APLICAÇÕES

3.69.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

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

3.69.3. Reconhecer pelo menos 3000 aplicações diferentes, incluindo, mas não limitado: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, atualização de software, protocolos de rede, VoIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail.

3.69.4. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443.

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

3.69.6. Deve permitir a utilização de aplicativos para um determinado grupo de usuários e bloquear para o restante, incluindo, mas não limitado a Skype. Deve permitir também a criação de políticas de exceção, concedendo o acesso a aplicativos como Skype apenas para alguns usuários.

3.69.7. Identificar o uso de táticas evasivas via comunicações criptografadas.

3.69.8. Atualizar a base de assinaturas de aplicações automaticamente.

3.69.9. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD.

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

3.69.11. Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente à possibilidade de habilitar controle de aplicações em algumas regras.

3.69.12. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística.

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

3.69.14. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão.

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

3.69.16. Deve alertar o usuário quando uma aplicação for bloqueada.

3.69.17. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações.

3.69.18. Deve permitir criar filtro na tabela de regras de segurança para exibir somente:

3.69.19. Regras que permitem a passagem de tráfego baseado na porta e não por aplicação, exibindo quais aplicações estão trafegando nas mesmas, o volume em bytes trafegado por cada aplicação pelos últimos 30 dias e o primeiro e último registro de log de cada aplicação trafegada por esta determinada regra.

3.69.20. Aplicações permitidas em regras de forma desnecessária, pois não há tráfego da mesma na determinada regra.

3.69.21. Regras de segurança onde não houve passagem de tráfego nos últimos 90 dias.

## 3.70. PREVENÇÃO DE AMEAÇAS

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

3.70.2. Deve ter a capacidade de bloquear ameaças desconhecidas em tempo real.

3.70.3. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado com a última base de assinatura instalada no momento em que a licença expirou, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

3.70.4. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo.

3.70.5. As assinaturas podem ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração.

3.70.6. Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura.

3.70.7. Deve permitir o bloqueio de vulnerabilidades.

3.70.8. Deve permitir o bloqueio de exploits conhecidos.

3.70.9. Deve incluir proteção contra-ataques de negação de serviços.

3.70.10. Deverá possuir os seguintes mecanismos de inspeção de IPS:

3.70.11. Análise de padrões de estado de conexões.

3.70.12. Análise de decodificação de protocolo.

3.70.13. Análise para detecção de anomalias de protocolo.

3.70.14. Análise heurística.

3.70.15. IP Defragmentation.

3.70.16. Remontagem de pacotes de TCP.

3.70.17. Bloqueio de pacotes malformados.

3.70.18. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPflood etc.

3.70.19. Detectar e bloquear a origem de port scans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização.

3.70.20. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador

acrescentar novos padrões.

3.70.21. Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados.

3.70.22. Possuir assinaturas específicas para a mitigação de ataques DoS.

3.70.23. Possuir assinaturas para bloqueio de ataques de buffer overflow.

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

3.70.25. Identificar e bloquear comunicação com botnets.

3.70.26. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

3.70.27. O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.

3.70.28. Deve suportar a captura de pacotes (PCAP), por assinatura de Malware e aplicação.

3.70.29. Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3.

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

3.70.31. Deve incluir proteção contra vírus em conteúdo HTML e JavaScript, software espião (spyware) e worms.

3.70.32. Bloquear proativamente os ataques sofisticados recém-descobertos em tempo real com IA e serviços avançados de proteção contra ameaças.

3.70.33. Proteção contra downloads involuntários usando HTTP de arquivos executáveis.

3.70.34. Rastreamento de vírus em PDF.

3.70.35. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.).

## 3.71. FILTRO DE URL

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

3.71.2. Deve ter a capacidade de bloquear ameaças desconhecidas em tempo real.

3.71.3. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado com a última base de assinatura instalada no momento em que a licença expirou, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

3.71.4. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo.

3.71.5. As assinaturas podem ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração.

3.71.6. Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura.

3.71.7. Deve permitir o bloqueio de vulnerabilidades.

3.71.8. Deve permitir o bloqueio de exploits conhecidos.

3.71.9. Deve incluir proteção contra-ataques de negação de serviços.

3.71.10. Deverá possuir os seguintes mecanismos de inspeção de IPS:

3.71.11. Análise de padrões de estado de conexões.

3.71.12. Análise de decodificação de protocolo.

3.71.13. Análise para detecção de anomalias de protocolo.

3.71.14. Análise heurística.

3.71.15. IP Defragmentation.

3.71.16. Remontagem de pacotes de TCP.

3.71.17. Bloqueio de pacotes malformados.

3.71.18. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPflood, etc.

3.71.19. Detectar e bloquear a origem de port scans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização.

3.71.20. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões.

3.71.21. Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de

padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados.

3.71.22. Possuir assinaturas específicas para a mitigação de ataques DoS.

3.71.23. Possuir assinaturas para bloqueio de ataques de buffer overflow.

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

3.71.25. Identificar e bloquear comunicação com botnets.

3.71.26. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

3.71.27. O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.

3.71.28. Deve suportar a captura de pacotes (PCAP), por assinatura de Malware e aplicação.

3.71.29. Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3.

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

3.71.31. Deve incluir proteção contra vírus em conteúdo HTML e JavaScript, software espião (spyware) e worms.

3.71.32. Bloquear proativamente os ataques sofisticados recém-descobertos em tempo real com IA e serviços avançados de proteção contra ameaças.

3.71.33. Proteção contra downloads involuntários usando HTTP de arquivos executáveis.

3.71.34. Rastreamento de vírus em PDF.

3.71.35. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.).

## 3.72. PREVENÇÃO DE AMEAÇAS AVANÇADAS (ZERO DAY)

3.72.1. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado.

3.72.2. Deve ser capaz de enviar para análise, arquivos do tipo Executáveis, DLLs, Arquivos de Código e MSI.

3.72.3. A solução deve detectar e bloquear em tempo real (inline) os artefatos maliciosos desconhecidos (zero day) no próprio gateway através de mecanismos de Machine Learning.

3.72.4. Suportar a análise dinâmica de arquivos maliciosos em ambiente controlado com, no mínimo, os sistemas operacionais Windows XP, Windows 7, Windows 10, Mac OS X, Android e Linux.

3.72.5. A análise de links em sandbox deve ser capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução.

3.72.6. Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência.

3.72.7. Deve permitir o download dos malwares identificados a partir da própria interface de gerência.

3.72.8. Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados.

3.72.9. Deve permitir informar ao fabricante quanto à suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia Zero a partir da própria interface de gerência.

3.72.10. Caso sejam necessárias licenças de sistemas operacionais e softwares para execução de arquivos no ambiente controlado (sandbox), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante.

3.72.11. Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado.

3.72.12. Suportar a análise de arquivos do pacote Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos Java (.jar e .class), Android APKs, MacOS (Mach-O, DMG e PKG), Linux (ELF), RAR e 7-ZIP no ambiente de sandbox.

3.72.13. A solução deve analisar os arquivos do tipo malware em bare-metal para evitar técnicas de evasão. Caso não possua essa funcionalidade, será permitido a integração com ferramentas que executam esta função. No caso de equipamento físico (appliance) do próprio fabricante, devem ser fornecidas no mínimo 28 máquinas virtuais (VM) simultaneamente por appliance.

3.72.14. As funcionalidades de sandbox têm como objetivo analisar e bloquear em tempo real Ameaças Avançadas Persistentes (APT). Essas funcionalidades têm o objetivo de proteger o ambiente contra a entrada de malwares não conhecidos, e para que sejam efetivas, é necessário que a inspeção e bloqueio sejam feitas em linha (inline), através de features de machine learning.

3.72.15. Permitir o envio de arquivos e links para análise no ambiente controlado de forma automática via API.

3.72.16. Deve permitir o envio para análise em sandbox de malwares bloqueados pelo antivírus da solução.

3.72.17. A solução deve analisar os arquivos do tipo malware em bare metal para evitar técnicas de evasão. Caso não possua essa funcionalidade, será permitido a integração com ferramentas que executam esta função.

3.72.18. Deve prevenir contra-ataques sem arquivo, buscando por atividade maliciosa em pelo menos nas seguintes linguagens de scripts: PowerShell e JavaScript.

3.72.19. Deve ser capaz de aplicar, de forma complementar às assinaturas de antivírus, a inspeção inline através de Machine Learning em tempo real em arquivos do tipo PE (Portable

Executable), ELF (Executable and Linked Format) e Arquivos Microsoft Office, bem como scripts PowerShell e shell script em tempo real para malwares desconhecidos.

3.72.20. A solução de prevenção de ameaças deve identificar e bloquear links maliciosos dentro de e-mails (SMTP e POP3).

## 3.73. IDENTIFICAÇÃO DE USUÁRIOS

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

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

3.73.3. Deve possuir integração com RADIUS para identificação de usuários e grupos, permitindo granularidade de controle e políticas baseadas em usuários e grupos de usuários.

3.73.4. Deve possuir integração com LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.

3.73.5. Deve suportar o recebimento de eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via syslog, para a identificação de endereços IP e usuários.

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

3.73.7. Suporte à autenticação Kerberos.

3.73.8. Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, Captive Portal e usuários de VPN SSL.

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

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

## 3.74. SOLUÇÃO DE SEGURANÇA PARA DNS

3.74.1. A solução deve mostrar nos logs as seguintes informações sobre domínios DGA:

3.74.2. Domínio suspeito identificado.

3.74.3. ID de assinatura de detecção.

3.74.4. Usuário logado na estação/servidor que originou o tráfego.

3.74.5. Aplicação.

3.74.6. Porta de destino.

3.74.7. IP de origem.

3.74.8. IP de destino.

3.74.9. Horário.

3.74.10. Ação do firewall.

3.74.11. Severidade.

3.74.12. A solução deve possuir sistema de análise automático para detectar e bloquear encapsulamento de DNS com fins de roubo de dados e comunicações de comando e controle.

3.74.13. A análise automática deve incluir, no mínimo, as seguintes características:

3.74.14. Padrões de consulta.

3.74.15. Entropia.

3.74.16. Análise de frequência n-gram de domínios.

3.74.17. Taxa de consultas.

## 3.75. QoS

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

3.75.2. Suportar a criação de políticas de QoS por:

3.75.3. Endereço de origem.

3.75.4. Endereço de destino.

3.75.5. Por usuário e grupo do LDAP/AD.

3.75.6. Por aplicações.

3.75.7. Por porta.

3.75.8. O QoS deve possibilitar a definição de classes por:

3.75.9. Banda Garantida.

3.75.10. Banda Máxima.

3.75.11. Fila de Prioridade.

3.75.12. Suportar priorização Real-Time de protocolos de voz (VoIP), como H.323, SIP, SCCP, MGCP e aplicações como Skype.

3.75.13. Suportar marcação de pacotes Diffserv, inclusive por aplicação.

3.75.14. Deve implementar QoS (traffic-shaping) para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (inbound e outbound).

3.75.15. Disponibilizar estatísticas Real-Time para classes de QoS.

3.75.16. Deve suportar QoS (traffic-shaping) em interfaces agregadas.

3.75.17. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

## 3.76. VPN

3.76.1. A solução de VPN client-to-site deverá ser atendida apenas para o equipamento do tipo II.

3.76.2. Suportar VPN Site-to-Site e Client-To-Site.

3.76.3. Suportar IPSec VPN.

3.76.4. Suportar SSL VPN.

3.76.5. A VPN IPSec deve suportar:

3.76.6. 3DES.

3.76.7. Autenticação MD5 e SHA-1.

3.76.8. Diffie-Hellman Group 1, Group 2, Group 5 e Group 14.

3.76.9. Algoritmo Internet Key Exchange (IKEv1 e v2).

3.76.10. AES 128 e 256 (Advanced Encryption Standard).

3.76.11. Autenticação via certificado IKE PKI.

3.76.12. Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSec a partir da interface gráfica da solução, facilitando o processo de troubleshooting.

3.76.13. Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, Anti-Spyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL.

3.76.14. Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local.

3.76.15. Deve suportar a distribuição de certificado para o usuário remoto através do portal de VPN de forma automatizada.

3.76.16. Deve suportar a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL.

3.76.17. O cliente da solução de VPN client-to-site deve suportar a instalação nos seguintes tipos de sistemas operacionais:

3.76.18. Microsoft Windows.

3.76.19. Apple macOS e iOS.

3.76.20. Android.

3.76.21. Linux.

3.76.22. A solução de VPN *client-to-site* deve estar devidamente licenciada para criar perfis customizados de conformidade dos clientes das VPNs *client-to-site* para, no mínimo, as seguintes opções:

3.76.23. Sistema operacional.

3.76.24. Antivírus instalado.

3.76.25. Firewall no host.

3.76.26. Chaves de registros (quando aplicável).

3.76.27. Processos ativos.

3.76.28. Os mecanismos de conformidade da solução de VPN client-to-site deverão monitorar durante a conexão do usuário remoto qualquer tipo de atividade não autorizada pelo administrador em tempo real. Por exemplo: após o usuário ser conectado e admitido pela VPN client-to-site, o seu acesso ao ambiente corporativo pode ser negado caso ele manualmente desative alguma funcionalidade especificada nos testes de conformidade da solução.

3.76.29. Deve haver a opção do cliente remoto escolher manualmente o gateway de VPN e, de forma automática, através da melhor rota entre os gateways disponíveis com base no tempo de resposta mais rápido.

## 3.77. SERVIÇO DE PROTEÇÃO DE ENDPOINTS/SERVIDORES

### 3.77.1. FUNCIONALIDADES GERAIS

3.77.1.1. Deve ser ofertado pacotes de até 150 ativos.

3.77.1.2. Será responsabilidade da CONTRATADA arcar com todos os custos referentes aos recursos, sem nenhum ônus financeiro ou vínculo empregatício para a CONTRATANTE.

3.77.1.3. A entidade requer uma solução de Extended Detection & Response, tecnologia que amplia as capacidades de detecção e resposta além de soluções de endpoints tradicionais (EDR, Antivírus e EPP).

3.77.1.4. A solução deve ser capaz de ingerir dados de identidade do usuário, armazenando e correlacionando todas essas informações em um único data lake para que, por meio de

algoritmos automatizados, os analistas possam identificar anomalias e detectar problemas em tempo hábil.

3.77.1.5. A tecnologia deve incluir ações de resposta a incidentes em endpoints e permitir integração com soluções SOAR (Security Orchestration Automation & Response).

3.77.1.6. A solução deve ter participado das rodadas de detecção MITRE ATT&CK e deve ter participado do teste de detecção e proteção do ano de 2023, no relatório mais recente do MITRE ENGENUITY (https://attackevals.mitre-engenuity.org/), que serão utilizados para avaliar os recursos tecnológicos de detecção e defesa apresentados pelos fabricantes. A classificação preferencial será "Technique", não sendo válidos recursos que tiveram resultados classificados como "None".

3.77.1.7. Recursos tecnológicos para detecção e defesa testados no relatório mais recente do MITRE ENGENUITY (https://attackevals.mitre-engenuity.org/) classificados acima de "None", preferencialmente em "Technique", para os tipos de ataque: Email Hiding Rules, Traffic Signaling, Drive-by Compromise, Command and Scripting Interpreter: PowerShell, Deobfuscate/Decode Files or Information, Rootkit, Event Triggered Execution, Indicator Removal: File Deletion, Email Collection: Remote Email Collection e Exfiltration Over C2 Channel.

3.77.1.8. A ferramenta de endpoint XDR deve possuir a capacidade de apresentar informações de telemetria do dispositivo (computadores e servidores) que têm o agente instalado, mesmo que esse endpoint não apresente alertas ou incidentes de segurança.

### 3.77.2. Prevenção contra Técnicas de Exploração de Vulnerabilidade.

3.77.2.1. A solução de Endpoint XDR deve possuir na sua console de gerenciamento centralizado a matriz do MITRE ATT&CK como padrão na apresentação de técnicas de exploração.

3.77.2.2. Detecção e prevenção do mecanismo de identificação das propriedades de um sistema por um Exploit Kit (técnica conhecida como Exploit Kit Fingerprint) sem a necessidade de usar assinaturas, padrões ou heurísticas.

3.77.2.3. Detecção de técnicas de exploração sem a necessidade de uso de assinaturas, padrões ou heurísticas, principalmente focadas na prevenção de exploits lógicos, processos vulneráveis e exploits de sistema operacional para sistemas Microsoft Windows.

3.77.2.4. Mitigação de vulnerabilidades conhecidas, desconhecidas e de dia zero.

3.77.2.5. Suporte à identificação de diferentes técnicas de exploração de vulnerabilidades, entre as quais Return Oriented Programming (ROP), Heap Spray, Jit Spray, Shpell link, Structured Exception Handler (SEH), etc.

3.77.2.6. Proteção de aplicativos contra técnicas de exploração por padrão e de forma nativa.

3.77.2.7. Entre os aplicativos protegidos por padrão devem estar: Firefox, Internet Explorer, Microsoft Word, Microsoft Excel, várias versões do Flash Player, Microsoft Silverlight, Apache, IIS, entre outros.

3.77.2.8. Capacidade de usar módulos de proteção contra técnicas de exploração em qualquer aplicação ou processo, incluindo aqueles desenvolvidos internamente.

3.77.2.9. Capacidade de criar automaticamente um snapshot da memória RAM ao impedir a execução de uma técnica de exploração, a fim de fornecer dados forenses sobre o evento.

3.77.2.10. Capacidade de realizar análise avançada do status da memória quando um alerta de prevenção de exploração é gerado.

3.77.2.11. Permitir a configuração de perfis de proteção em modo de prevenção ou monitoramento.

3.77.2.12. Capacidade de encerramento do processo em que foi identificada a tentativa de execução de uma técnica de exploração, desde que não seja um processo crítico do sistema operacional.

3.77.2.13. Prevenção de técnicas de exploração usando Dylib-Hijacking para Mac OS.

3.77.2.14. Prevenção de técnicas de exploração usando Return Oriented Program (ROP) para Mac OS.

3.77.2.15. Prevenção de técnicas de exploração usando JIT para Mac OS.

3.77.2.16. Prevenção de técnicas de exploração que buscam sequestrar o fluxo de controle de um processo, monitorando tentativas de enumeração de alocação de memória para sistemas operacionais Linux.

3.77.2.17. Prevenção de técnicas de exploração que buscam redirecionar fluxos de entrada e saída padrão para soquetes de rede para sistemas operacionais Linux.

3.77.2.18. Prevenção de técnicas de exploração que usam Return Oriented Program (ROP) para sistemas operacionais Linux.

3.77.2.19. Prevenção do uso de certas áreas de memória que são comumente utilizadas para armazenar payload de um ataque baseado em técnicas de heap spray, para sistemas operacionais Linux.

3.77.2.20. Proteção contra ataques de webshells de PHP em servidores Linux.

3.77.2.21. Capacidade de fornecer proteção contra ataques que utilizam técnicas de exploração de vulnerabilidades sem exigir que a máquina protegida possua uma conexão com o console de gerenciamento.

3.77.2.22. A solução deve ter a capacidade de detecção e prevenção contra-ataques cibernéticos mesmo que o agente instalado no dispositivo (computadores e servidores) não tenha conexão com o console de gerenciamento centralizado e com a Internet.

3.77.2.23. Análise de identidade para detectar ameaças baseadas no usuário, como movimento lateral.

3.77.2.24. A solução deve identificar comportamento que caracteriza uma quantidade excessiva de logins.

3.77.2.25. A solução deve possuir um módulo que seja capaz de identificar Brute Force em usuário e senha.

3.77.2.26. A solução deve apresentar escore de risco de segurança para cada usuário com o agente instalado.

### 3.77.3. Identificação de ataques de pós-exploração.

3.77.3.1. A solução de Endpoint XDR deve possuir na sua console de gerenciamento centralizado a matriz do MITRE ATT&CK como padrão para detalhar as ações técnicas utilizadas na exploração.

3.77.3.2. Identificação e prevenção de tentativas de escalar privilégios no nível do Kernel. Essa proteção deve poder ser usada em agentes instalados em endpoints com Sistemas Operacionais Windows, Mac e Linux.

3.77.3.3. Detecção e encerramento de comportamentos considerados maliciosos através da análise contínua da cadeia de eventos que ocorrem em um endpoint. Essa detecção deve considerar vários eventos e não apenas um evento para fornecer um veredicto de atividade maliciosa. A detecção deve utilizar várias regras pré-configuradas, que devem ter a capacidade de analisar vários eventos e não apenas um evento.

3.77.3.4. A proteção não deve exigir uma conexão da máquina protegida com a console de gerenciamento.

### 3.77.4. Prevenção contra malware conhecido.

3.77.4.1. Deve fornecer proteção na memória contra o uso do Mimikatz ou ferramenta de extração de senha semelhante.

3.77.4.2. Geração de hashes de processos em execução e verificação de veredictos em uma nuvem de inteligência de ameaças.

3.77.4.3. Envio de executáveis, quando seu hash é desconhecido, para análise em um sandbox localizado na nuvem, a fim de determinar se são maliciosos ou benignos. Essa proteção deve estar disponível para os sistemas operacionais Windows, Mac, Linux e Android.

3.77.4.4. Capacidade de prevenir contra ataques de shell reversos (Reverse Shell) para sistemas operacionais Linux.

3.77.4.5. Capacidade de escanear o computador comparando os hashes dos arquivos executáveis que estão armazenados no computador com a base de veredictos em uma nuvem de inteligência de ameaças.

3.77.4.6. Capacidade de enviar arquivos classificados como maliciosos para quarentena, sejam eles identificados no momento da tentativa.

3.77.4.6. Capacidade de enviar arquivos classificados como maliciosos para quarentena, sejam eles identificados no momento da tentativa de execução ou no momento da identificação por meio de uma varredura.

3.77.4.7. Deve ter um módulo de prevenção de ransomware, que deve impedir um processo de criptografia identificando tentativas de modificação de arquivos.

3.77.4.8. Capacidade de proteção contra-ataques de mineração de bitcoin para dispositivos Linux, detectando-os por seu comportamento e não somente assinatura de hash.

### 3.77.5. Prevenção contra malware desconhecido.

3.77.5.1. Deve usar um modelo matemático gerado a partir de aprendizado de máquina para comparar um grande número de características de um arquivo executável, de forma estática,

para determinar se ele é malicioso. Essa proteção deve estar disponível para os sistemas operacionais Windows, Linux e Mac.

3.77.5.2. Deve permitir a criação de listas de bloqueio de arquivos a partir de seu hash para que o administrador possa determinar quais aplicativos podem ser executados no ambiente.

3.77.5.3. Capacidade de identificar se a macro contida em um documento do Word ou Excel é maliciosa, sem precisar executar a macro ou observar seu comportamento ou execução, para determinar se é maliciosa.

3.77.5.4. Capacidade de proteção contra malware sem a necessidade de assinaturas, padrões e/ou heurísticas.

3.77.5.5. Deve ser possível configurar as políticas em modo de prevenção ou monitoramento.

3.77.5.6. Deve permitir que os arquivos detectados como maliciosos sejam colocados em quarentena, automaticamente ou sob demanda.

3.77.5.7. Envio de arquivos desconhecidos de forma automática para um sandbox para serem analisados, adicionalmente a todos os recursos de detecção/bloqueio local no agente em execução no Windows, Linux e MacOS, e permitir visualizar os relatórios de análise detalhados e baixá-los a qualquer momento no console.

3.77.5.8. A solução de Sandbox deve enviar automaticamente artefatos para inspeção em sua sandbox com tamanho de até 100Mb.

3.77.5.9. A solução não deve possuir limitação na quantidade de artefatos ou consultas que deverão ser enviados para a Sandbox. Caso tenha alguma limitação, deverá ser considerado o maior volume de créditos/licenciamento para inspeção de objetos e URLs suspeitas, sem gerar nenhum tipo de prejuízo em caso de alta demanda de inspeção de artefatos suspeitos.

3.77.5.10. Deve prover solução de Sandbox do mesmo fabricante da solução, baseada em pelo menos uma das seguintes plataformas:

3.77.5.10.1. Máquinas virtualizadas.

3.77.5.10.2. Máquinas Bare Metal.

3.77.5.10.3. Cloud.

3.77.5.11. Envio de executáveis, quando seu hash é desconhecido, para análise em um sandbox localizado na nuvem, a fim de determinar se são maliciosos ou benignos. Essa proteção deve estar disponível para os sistemas operacionais Windows, Mac, Linux e Android.

3.77.6. Scan periódico/sob demanda de arquivos executáveis.

3.77.6.1. Permite a verificação de arquivos executáveis sem a necessidade de assinaturas.

3.77.6.2. Permite agendar a verificação de arquivos semanal ou mensalmente.

3.77.6.3. Permite definir o dia e a hora em que a verificação será iniciada.

3.77.6.4. O consumo de recursos no momento da verificação não deve afetar a experiência do usuário.

3.77.6.5. Permite habilitar a verificação de dispositivos de armazenamento removíveis.

3.77.6.6. Permite criar listas de exceção (Allow List) de pastas para que sejam excluídas do processo de verificação.

3.77.6.7. Permite que arquivos identificados como maliciosos sejam colocados em quarentena, se a política estiver configurada dessa forma.

3.77.6.8. Deve permitir que o usuário, a qualquer momento, inicie o scan de um arquivo presente no disco rígido de forma manual.

3.77.6.9. O scan de arquivos deve ser capaz de realizar análise estática em arquivos desconhecidos para determinar se eles são maliciosos, bem como enviar esses arquivos desconhecidos para o serviço de análise em nuvem.

### 3.77.7. Restrições de execução e exceções de política.

3.77.7.1. Deve permitir a criação de restrições na execução de arquivos de uma determinada pasta.

3.77.7.2. Deve permitir a criação de restrições na execução de arquivos de recursos compartilhados.

3.77.7.3. Deve permitir a criação de restrições na execução de arquivos de dispositivos USB ou CD/DVD.

3.77.7.4. Deve aplicar as restrições configuradas sem a necessidade de uma conexão com o console de gerenciamento.

3.77.7.5. Deve possuir políticas de restrição de criação de processo filho configuradas por padrão.

3.77.7.6. Deve permitir a criação de exceções para permitir a execução de arquivos de determinadas pastas.

3.77.7.7. Deve permitir a criação de exceções para permitir a execução de processos filho.

3.77.7.8. Deve permitir a criação de exceções para permitir a execução de arquivos de pastas em dispositivos de armazenamento removíveis.

3.77.7.9. Deve permitir a criação de políticas de restrição em modo de bloqueio ou apenas monitoramento.

### 3.77.8. Restrição do uso de mídias removíveis.

3.77.8.1. A solução deve ter a capacidade de permitir e bloquear o uso de discos removíveis para os tipos de dispositivos (computadores e servidores) nos sistemas operacionais Windows e MAC.

3.77.8.2. A solução deve ter a capacidade de permitir e bloquear o uso de discos removíveis através de políticas de segurança customizadas na gerência centralizada da solução de XDR.

3.77.8.3. Deve permitir a geração de perfis que gerenciam as seguintes características de bloqueio de porta USB quando os seguintes tipos de dispositivos estiverem conectados: discos rígidos, unidades de CD-ROM externas conectadas por USB, dispositivos de armazenamento removíveis portáteis conectados por USB, disquetes externos com conexão USB, adaptadores de rede em formato USB.

3.77.8.4. Deve permitir a geração de perfis de exceção para poder conectar dispositivos a portas USB utilizando os seguintes parâmetros: tipo de dispositivo, tipo de permissão para atribuir (leitura/gravação ou somente leitura), fabricante (deve conter uma lista padrão), produto (deve conter uma lista padrão) e número de série. O tipo de dispositivo, tipo de licença e parâmetros do fabricante devem ser obrigatórios.

3.77.8.5. Deve permitir a criação de políticas que utilizem os perfis de bloqueio e exceção por grupo de máquinas ou de forma global.

3.77.8.6. As políticas geradas devem poder ser atribuídas a um determinado computador ou a um grupo de computadores previamente definido.

3.77.8.7. Deve permitir a criação de exceções permanentes usando os seguintes parâmetros: tipo de dispositivo, tipo de permissão para atribuir, fabricante, produto e número de série. Essas exceções permanentes não devem depender de serem aplicadas a uma política para entrar em vigor.

3.77.8.8. Deve permitir a criação de regras de exceção temporárias a partir de uma violação de política de uso de mídias removíveis detectada no console de administração.

3.77.8.9. Deve mostrar as violações de política que foram registradas, incluindo hora, computador, usuário, endereço IP, tipo de dispositivo, produto, fabricante e número de série do dispositivo que tentou se conectar.

3.77.8.10. Essa funcionalidade deve ser compatível com os sistemas operacionais Windows e Mac.

### 3.77.9. Firewall de host.

3.77.9.1. Essa funcionalidade deve ser compatível com os sistemas operacionais Windows e Mac.

3.77.9.2. Os seguintes recursos devem estar disponíveis para sistemas operacionais Windows:

3.77.9.3. Controle de todas as comunicações de entrada e saída usando endereços IP.

3.77.9.4. Permitir que as regras sejam aplicadas de acordo com a localização do dispositivo, por exemplo, que só se apliquem se estiverem na rede interna.

3.77.9.5. O produto deve ser capaz de determinar, por meio da configuração, se o dispositivo está dentro ou fora da organização.

3.77.9.6. A regra poderá especificar endereços locais ou remotos, bem como portas locais ou remotas. O protocolo também pode ser especificado dentro destas quatro opções: ICMP, TCP, UDP, ICMPv6.

3.77.9.7. As seguintes funcionalidades devem estar disponíveis para sistemas operacionais Mac:

3.77.9.8. Permitir habilitar ou desabilitar o firewall nativo do sistema operacional.

3.77.9.9. Permitir ou bloquear comunicações de rede de entrada.

3.77.9.10. Ativar o modo furtivo.

3.77.9.11. Criar exclusões por aplicativo para permitir ou bloquear especificamente programas usando a funcionalidade do sistema operacional conhecida como BundleID.

### 3.77.10. Dados de Telemetria de Endpoint.

3.77.10.1. O produto deve ser capaz de capturar, no mínimo, as seguintes ações no nível de terminal em sistemas operacionais Windows:

3.77.10.2. Processo executado, incluindo hora de início e tamanho do arquivo associado.

3.77.10.3. Atividades de criação, escrita, renomeação, exclusão, modificação e criação de links simbólicos de um arquivo.

3.77.10.4. Os seguintes parâmetros devem ser registrados quando os arquivos DLL são carregados: caminho completo, endereço base, id do processo ou thread que o está carregando, tamanho da imagem, assinatura, valores de hash calculados com os algoritmos MD5 e SHA256 da DLL, tamanho do arquivo e tempo de acesso ao arquivo.

3.77.10.5. Criação e encerramento de processos.

3.77.10.6. Injeções em threads de processo. ID do encadeamento pai, ID do encadeamento novo ou encerrado, processo que iniciou o encadeamento (se for um processo diferente).

3.77.10.7. Protocolos de rede: solicitações DNS e respostas UDP, conexão HTTP, desconexão HTTP, análise de proxy HTTP.

3.77.10.8. Estatísticas da rede. Volume no momento do envio por um link TCP e volume recebido por meio de um link TCP.

3.77.10.9. Definição ou exclusão de valores do registro. Criar, modificar, excluir, adicionar, restaurar e salvar chaves de registro.

3.77.10.10. Sessões do sistema operacional: login, logoff, conexão e desconexão, considerando os seguintes atributos: login interativo, id da sessão, estado da sessão e se a sessão é local ou remota.

3.77.10.11. Status do computador: inicialização, suspensão, reinicialização, com os seguintes atributos: nome do computador, versão do sistema operacional, domínio, status anterior e atual.

3.77.10.12. Logs de eventos do Windows.

3.77.10.13. O produto deve ser capaz de capturar, no mínimo, as seguintes ações no nível de endpoint em sistemas operacionais Mac:

3.77.10.14. Criar, escrever, excluir, renomear, alterar o caminho e abrir arquivos, com os seguintes atributos: caminho completo do arquivo modificado antes e depois de sua modificação. Geração de hashes com algoritmos SHA256 e MD5 para o arquivo após sua modificação.

3.77.10.15. Iniciando e parando processos, com os seguintes parâmetros: ID do processo para o processo pai, ID do processo, caminho completo, argumentos de linha de comando, nível de integridade para determinar se o processo está sendo executado com privilégios elevados, valores de hash calculados com os algoritmos MD5 e SHA256, detalhes da assinatura ou do certificado usado para assinar o arquivo.

3.77.10.16. O produto deve ser capaz de capturar, no mínimo, as seguintes ações no nível de terminal em sistemas operacionais Linux:

3.77.10.16.1. Para arquivos, ações de criação, abertura, gravação e exclusão, incluindo o caminho completo do arquivo e o hash do arquivo (para determinados arquivos e somente se o arquivo foi gravado). Copiar ou renomear os arquivos, incluindo os caminhos completos dos arquivos originais e modificados. Ações para alterar o proprietário (chown) e o modo (chmod) dos arquivos, incluindo o caminho completo do arquivo, bem como o novo proprietário ou novos atributos.

3.77.10.16.2. Processos. Criação de processos, com os seguintes atributos: ID do processo filho, ID do processo pai, caminho completo da imagem do processo, linha de comando do

processo, valores de hash calculados com os algoritmos SHA256 e MD5. Encerramento de processos, incluindo o ID do processo.

### 3.77.11. Inventário de aplicações e vulnerabilidades.

3.77.11.1. O produto deve ser capaz de gerar um inventário de aplicativos instalados em computadores com sistema operacional Windows.

3.77.11.2. O inventário de aplicativos deve mostrar os aplicativos instalados em computadores com o sistema operacional macOS.

3.77.11.3. O inventário de aplicativos deve mostrar os aplicativos instalados em computadores com sistema operacional Linux.

3.77.11.4. O produto deve obter automaticamente os seguintes detalhes dos computadores: usuários, grupos de usuários, correlação de usuários e grupos, serviços instalados, drivers, autoruns, unidades de armazenamento compartilhadas configuradas e drivers instalados.

3.77.11.5. Deve oferecer visibilidade em tempo real das vulnerabilidades existentes, que afetam tanto o sistema operacional quanto os aplicativos instalados.

3.77.11.6. Deve fornecer detalhes de CVEs, incluindo nível de gravidade e métricas com base no banco de dados de vulnerabilidades NIST.

3.77.11.7. Deve permitir que você pesquise todos os arquivos nos endpoints da sua organização e exclua um arquivo específico em tempo real.

### 3.77.12. Análise de alertas e investigação.

3.77.12.1. Deve ter uma console em nuvem que permita visualizar alertas gerados de diferentes fontes.

3.77.12.2. Deve ser capaz de exibir o número total de alertas e incidentes e deve incluir a capacidade de filtrar informações de forma flexível.

3.77.12.3. Deve permitir a criação de uma sequência gráfica que correlaciona alertas individuais para descrever a sequência de um ataque.

3.77.12.4. Deve apresentar informações específicas sobre cada processo envolvido na sequência do ataque.

3.77.12.5. Deve apresentar os dados relacionados ao perfil de comportamento e a execução de cada processo envolvido na cadeia do ataque.

3.77.12.6. Deve exibir um aviso quando um determinado executável, que faz parte da sequência gráfica, se comporta de forma suspeita.

3.77.12.7. Deve apresentar dados gerais da execução de um processo que faz parte da sequência gráfica, entre os quais estão caminho de execução, nome do usuário que executou o processo, tempo de execução, entidade que assinou o processo, valor MD5 do executável relacionado ao processo, veredicto de análise de sandbox, valor SHA256 e linha de comando de execução.

3.77.12.8. Deve mostrar a atividade de cada processo identificado, em colunas por categorias. As categorias a serem incluídas devem incluir atividade de rede, atividade de arquivo, atividade de registro, módulos executados e tentativas de injeção de processo.

3.77.12.9. Deve usar aprendizado de máquina supervisionado e não supervisionado para estabelecer linhas de base do comportamento típico do usuário e do dispositivo e detectar desvios comportamentais que caracterizam atividade anômala.

3.77.12.10. Deve fornecer a capacidade de descodificar cadeias de caracteres codificados em base 64, utilizadas em comandos de execução, para exibição em texto simples.

3.77.12.11. Deve ser capaz de identificar, de todas as atividades mencionadas acima, aquelas que são maliciosas ou altamente suspeitas e separá-las em uma categoria de fácil acesso ao analista.

3.77.12.12. Deve possuir inteligência de ameaças compartilhada para distribuir inteligência de ameaças de crowdsourcing do serviço de análise de malware baseado em nuvem para firewalls, agentes de endpoint e serviços de detecção e resposta.

3.77.12.13. Deve mostrar se houve injeção de código ou se o protocolo RPC é utilizado em outro processo a partir de um computador local ou remoto.

3.77.12.14. Deve fornecer graficamente a interação ocorrida com os endereços IP a serem investigados.

3.77.12.15. Deve ser capaz de mostrar diferentes opções de visualização, como localização geográfica ou os arquivos executáveis que geraram essa comunicação.

3.77.12.16. Deve fornecer graficamente a interação

3.77.12.16. Deve fornecer graficamente a interação que existe entre um ou vários processos investigados. O gráfico deve mostrar a interação entre os processos e se existe relação entre os computadores que executam tais processos, entre outros aspectos.

3.77.12.17. A solução deve possuir terminal remoto para acessar qualquer dispositivo (computadores Windows, Linux e MAC) para qualquer análise de processo, pastas e arquivos.

### 3.77.13. Gestão de Alertas e Incidentes.

3.77.13.1. Deve possuir mecanismos de geração de alertas considerando o comportamento apresentado pelos processos computacionais.

3.77.13.2. Os alertas gerados pelo comportamento dos processos não devem utilizar assinaturas ou heurísticas.

3.77.13.3. Cada alerta gerado pelo comportamento dos processos deve ter uma descrição do comportamento identificado.

3.77.13.4. Cada alerta gerado deve ter uma classificação de acordo com sua severidade.

3.77.13.5. Deve permitir que o analista crie regras de comportamento para geração de alertas.

3.77.13.6. Deve permitir a geração de exceções ao comportamento dos processos que foram identificados como maliciosos ou suspeitos.

3.77.13.7. Deve permitir desabilitar, modificar ou eliminar os comportamentos que geram os alertas devido ao comportamento dos processos.

3.77.13.8. Deve permitir a importação de regras de comportamento suspeito.

3.77.13.9. Deve suportar o uso de indicadores tradicionais de comprometimento, incluindo caminhos de arquivos, nomes de arquivos, domínios, endereços IP e hashes.

3.77.13.10. Deve permitir desabilitar, modificar, exportar ou deletar um indicador de comprometimento através de um menu de contexto.

3.77.13.11. Deve permitir o gerenciamento dos indicadores de comprometimento por comportamento de processo e indicadores tradicionais de comprometimento por meio da console de gerenciamento.

### 3.77.14. Ações de resposta.

3.77.14.1. A solução deve ter a capacidade de criação de regras de automação que irão executar comandos no dispositivo com o agente XDR instalado assim que um alerta de segurança for identificado.

3.77.14.2. Deve permitir que você isole um computador do próprio console de administração para que haja apenas comunicação entre o agente e o console. Deve oferecer a capacidade de adicionar comentários que expliquem por que um computador foi isolado.

3.77.14.3. Através da console centralizada da solução XDR, deve permitir a criação de regras customizadas pelo cliente para restringir a execução de softwares ou processos não autorizados nos computadores/servidores.

3.77.14.4. Deve permitir adicionar IPs a listas dinâmicas externas (EDL) para que possam ser consumidos por NGFWs ou outras tecnologias.

3.77.14.5. Deve definir outros processos e destinos (endereços IP) aos quais o computador pode se conectar, além do console, em caso de isolamento.

3.77.14.6. Deve colocar em quarentena, sob demanda, arquivos maliciosos que foram detectados ou alertados, mas não bloqueados por políticas de prevenção definidas.

3.77.14.7. Deve exibir os detalhes dos arquivos que foram colocados em quarentena.

3.77.14.8. Deve permitir a exportação de todos os detalhes dos arquivos que foram colocados em quarentena em um arquivo com formato “tab-separated value” (TSV).

3.77.14.9. Deve permitir a restauração de um ou mais arquivos que foram colocados em quarentena simultaneamente.

3.77.14.10. O produto deve permitir uma conexão reversa com o dispositivo afetado, em versões superiores ao Windows 7 SP1, por meio de uma conexão remota para permitir as seguintes ações:

3.77.14.11. Encerrar o processo de execução.

3.77.14.12. Suspender ou retomar o processo de execução.

3.77.14.13. Adicionar um processo a um indicador de comprometimento (IOC).

3.77.14.14. Cópia de binário em execução para investigação adicional.

3.77.14.15. Deve permitir uma conexão reversa com o dispositivo afetado por meio de uma conexão remota para permitir a execução de scripts ou comandos no Python versão 3, no mínimo.

3.77.14.16. Deve permitir uma conexão reversa com o dispositivo afetado por meio de uma conexão remota para permitir a execução de scripts ou comandos no PowerShell.

3.77.14.17. Deve permitir que unidades de armazenamento sejam acessadas remotamente, incluindo não apenas discos rígidos, mas também dispositivos de armazenamento removíveis. Deve permitir mover, renomear, excluir, baixar e fazer o hash de qualquer arquivo.

3.77.14.18. Deve permitir a criação de listas de permissão e bloqueio de execução de arquivos.

3.77.14.19. Deve adicionar as informações de incidentes associadas quando um arquivo estiver na lista de permissões ou na lista de bloqueio.

3.77.14.20. Deve apresentar recomendações de ações corretivas a serem adotadas no endpoint com base nos dados obtidos em alertas relacionados a ações suspeitas, permitindo a recuperação do ambiente a um estado prévio ao comprometimento.

3.77.14.21. Deve realizar automaticamente a restauração ou deleção de arquivos, pastas e chaves de registro selecionadas pelo analista na tela de recomendações de correção.

### 3.77.15. Gestão de políticas e eventos.

3.77.15.1. Gerenciamento centralizado de políticas, por meio de um console de gerenciamento em nuvem.

3.77.15.2. Deve identificar claramente os eventos que foram relatados e/ou bloqueados e os que foram detectados.

3.77.15.3. Deve classificar o status dos incidentes em quatro níveis diferentes de severidade: alto, médio, baixo e informativo.

3.77.15.4. Deve classificar o status dos alertas em quatro níveis diferentes de severidade: alto, médio, baixo e informativo.

3.77.15.5. Deve agrupar alertas relacionados em incidentes, bem como fornecer um contexto dos mesmos.

3.77.15.6. Deve extrair os elementos importantes ou relevantes dos alertas e exibi-los como um resumo na tela de análise de incidentes.

3.77.15.7. Deve fornecer informações detalhadas, sob demanda, dos eventos identificados como exploits.

3.77.15.8. Deve permitir a atualização e desinstalação do agente a partir da console de gerenciamento.

3.77.15.9. Deve permitir o uso de qualquer aplicativo de terceiros para poder instalar o agente.

3.77.15.10. Deve possuir integração com o Active Directory para gerenciamento do computador e configuração de políticas.

3.77.15.11. Deve ter a capacidade de criar perfis granulares.

3.77.15.12. Deve ter a capacidade de criar políticas com base nos grupos de máquinas criados.

3.77.15.13. Deve ter a capacidade de aplicar políticas a usuários, grupos, computadores ou unidades organizacionais do Active Directory.

3.77.15.14. Deve ter a capacidade de criar grupos virtuais que podem ser alimentados de forma estática e dinâmica.

3.77.15.15. Cada evento de prevenção ou alerta deve possuir informações básicas como tipo de evento, módulo que realizou a prevenção, detalhes daquele módulo, nome do computador, nome de usuário, sistema operacional, versão do agente, processo que gerou o evento de prevenção, rota de execução do processo que gerou o evento de prevenção (se disponível), hora e data do evento, informação forense (se disponível).

3.77.15.16. Deve ser fornecido sob um licenciamento de software como serviço (SaaS).

3.77.15.17. Deve possuir um dashboard mostrando os incidentes de segurança que não foram atendidos (classificados de acordo com sua criticidade em alta, média e baixa), um resumo dos incidentes de segurança, o número de endpoints que possuem o agente instalado (classificado para sua plataforma) e a versão do agente.

3.77.15.18. Deve possuir um dashboard onde são descritas as características dos incidentes de segurança que foram gerados. Este dashboard deve permitir uma análise mais detalhada dos alertas de segurança.

3.77.15.19. Deve permitir a criação de exceções a regras, mecanismos de detecção e/ou mecanismos de proteção a partir do console. Essas exceções devem ser aplicáveis a um computador específico ou a um grupo de computadores.

3.77.15.20. Características do Agente

3.77.15.20.1. Agente com footprint mínimo que não afeta a experiência do usuário.

experiência do usuário.

3.77.15.20.2. Pouco armazenamento em disco devido ao fato de não utilizar assinaturas, padrões e/ou heurísticas.

3.77.15.20.3. Suporte para as seguintes versões de sistemas operacionais:

3.77.15.20.4. Windows 10 Pro (32-bit e 64-bit), Windows 10 Enterprise LTSB, Windows versão 10, Windows Server 2012 (todas as edições; FIPS mode), Windows Server 2012 R2 (todas as edições), Windows Server 2016, Windows Server 2016 Datacenter, Windows Server 2019 Standard (Server Core), Windows Server 2022.

3.77.15.20.5. macOS 10.13 (High Sierra) e outros acima.

3.77.15.20.6. CentOS 6, CentOS 7, Red Hat Enterprise Linux 6, Red Hat Enterprise Linux 7, Suse for Enterprise 11, Suse for Enterprise 12, Suse for Enterprise 15, Ubuntu Server 12, Ubuntu Server 14, Ubuntu Server 16, Ubuntu Server 18, Ubuntu Server 20, Ubuntu 22.04 LTS.

3.77.15.20.7. A console deve permitir a criação do arquivo do agente de acordo com o sistema operacional.

3.77.15.20.8. Através da solução de gerenciamento, deve ser possível verificar qual versão do agente está aplicada para determinado computador.

3.77.15.20.9. Capacidade de agrupamento de máquinas por características comuns entre as mesmas, por exemplo: agrupar máquinas com o mesmo sistema operacional, agrupar máquinas no mesmo range de IP, agrupar máquinas com a mesma OU no Active Directory, etc.

### 3.77.15.21. Threat Hunting.

3.77.15.21.1. Deve permitir pesquisar, agendar e salvar consultas para identificar ameaças.

3.77.15.21.2. Deve oferecer recursos de busca flexíveis que permitam descobrir ameaças usando um construtor de consultas intuitivo, além de criar consultas avançadas e exibir resultados de maneira ordenada.

3.77.15.21.3. Deve contextualizar automaticamente as ameaças usando inteligência de ameaças.

3.77.15.21.4. Deve criar regras personalizadas de detecção de pesquisa de produtos e procurar manualmente por adversários emergentes usando os recursos de exploração de dados do produto.

3.77.15.21.5. Deve investigar ameaças e determinar o escopo completo dos incidentes.

3.77.15.21.6. Deve produzir relatórios detalhados de ameaças que revelam ferramentas de ataque e etapas para erradicar os adversários rapidamente.

3.77.15.21.7. Receber informações dos endpoints (Telemetria), de processos, comandos executados na máquina, informações de usuário e senha, mesmo antes da ocorrência de um alerta ou incidente.

3.77.15.21.8. Possibilidade de criar relatórios e dashboards com base em informações específicas do cliente, além do padrão da ferramenta.

3.77.15.21.9. Deve oferecer assistência direta para responder a perguntas e fornecer orientação sobre relatórios de ameaças e relatórios de impacto.

3.77.15.21.10. No momento de investigação, é de extrema importância a visibilidade da cadeia de todo o incidente, sendo que a gerência centralizada deverá apresentar o fluxo do ataque através de interface gráfica, detalhando os dispositivos envolvidos, estejam eles on-premises ou em cloud pública.

3.77.15.21.11. A gerência centralizada, através de sua interface gráfica, deverá apresentar os usuários e seus devidos níveis de riscos cibernéticos. Este nível de risco é calculado no volume de alertas, incidentes e características técnicas do usuário.

3.77.15.21.12. A gerência centralizada, através de sua interface gráfica, deverá apresentar os usuários e seus devidos níveis de riscos cibernéticos através de uma linha de tempo que pode ser configurada com data de início e fim para análises de comportamento.

3.77.15.21.13. Geração de hashes de processos em execução e verificação de veredictos em uma nuvem de inteligência de ameaças.

3.77.15.21.14. Deve identificar e apresentar graficamente através de console centralizada, tentativas de descoberta da senha do usuário (ex.: Brute Force) quando integrado com servidores de domínio Active Directory.

### 3.77.16. Correlação de eventos de segurança.

3.77.16.1. A solução deve ser capaz de ingerir alertas de qualquer marca de Firewall, incorporando-os aos incidentes existentes, oferecendo maior contexto ao analista durante a investigação.

3.77.16.2. A solução deve ser capaz de capturar logs de rede e, em conjunto com os dados do endpoint, deve gerar perfis comportamentais usando algoritmos supervisionados e não supervisionados.

3.77.16.3. Deve detectar uma tentativa de exfiltração automatizada identificando scripts AutoIt que fazem conexões com domínios externos.

3.77.16.4. Deve detectar tentativas de exfiltração por meio do encapsulamento de DNS.

3.77.16.5. Deve detectar tentativas de Discovery, destacando conexões com falha de um dispositivo para outro.

3.77.16.6. Deve detectar tentativas de comunicação de C2 (Command & Control), identificando resoluções para domínios criados por DGAs, destacando desvios no comportamento de resolução de DNS de um dispositivo.

3.77.16.7. Deve destacar tentativas de comunicação C2 (Command & Control), identificando binários legítimos ou "Living off the Land" executados por programas do Office que fazem conexões suspeitas com a Internet.

3.77.16.8. Deve destacar comandos e controles internos, identificando binários legítimos ou "Living off the Land" executados pelo Unix fazendo conexões suspeitas com a internet.

3.77.16.9. Deve identificar exfiltração de dados, destacando grandes quantidades de informações de um dispositivo via tráfego HTTP, FTP ou SMTP.

3.77.16.10. Deve identificar tentativas de comunicação com C2 (Command & Control) e evasão, destacando processos suspeitos simulando o navegador e outros processos válidos.

3.77.16.11. Deve destacar tentativas de comunicação com C2 (Command & Control), destacando dinamicamente conexões esporádicas a domínios DNS.

3.77.16.12. Deve identificar tentativas de comunicação com C2 (Command & Control), destacando conexões suspeitas com domínios de terceiros a partir de processos não assinados.

3.77.16.13. Deve identificar tentativas de comunicação com C2 (Command & Control), destacando conexões suspeitas com domínios categorizados como maliciosos recursivamente.

3.77.16.14. Deve identificar tentativas de comunicação com C2 (Command & Control), destacando conexões recursivas específicas para endereços IP externos.

3.77.16.15. Deve destacar as técnicas e táticas de ataque de acordo com a estrutura MITRE ATT&CK.

## 3.78. CAPACIDADE DE DETECÇÃO BASEADA EM NGFW

3.78.1. A solução deve ser capaz de ingerir alertas de rede de qualquer marca de Firewall, incorporando-os aos incidentes encontrados, oferecendo maior contexto ao analista durante a investigação;

3.78.2. A solução deve ser capaz de capturar logs de rede e, em conjunto com os dados do endpoint, deve gerar perfis comportamentais usando algoritmos supervisionados e não supervisionados;

3.78.3. Deve destacar quando um usuário, serviço ou conta de administrador tentar autenticar em recursos da rede, utilizando NTLM, de forma excessiva e em um curto espaço de tempo;

3.78.4. Deve identificar a tentativa de coleta de credenciais NTLM, destacando um número incomum de usuários tentando se autenticar em um destino na última hora;

3.78.5. Deve identificar varreduras de porta e reconhecimento, destacando quando um endpoint se conectou ou tentou se conectar a várias portas (Portas baixas), que raramente são usadas por outros endpoints;

3.78.6. Deve identificar quando um host procura se registrar como um novo controlador de domínio e alertar quando houver tráfego de sincronização de dados de um controlador de domínio legítimo;

3.78.7. Deve alertar a identificação de um processo conectando a uma porta padrão do Meterpreter;

3.78.8. Deve identificar quando um usuário tenta se autenticar em um host via NTLM e não o fez nos últimos 30 dias.

3.79. Capacidade de detecção baseada em dados de identidade

3.79.1. A solução deve ter a capacidade de ingerir dados de identidade de fontes como Azure AD, Okta ou PingOne;

3.79.2. Deve identificar quando um usuário desativado tenta autenticar;

3.79.3. Deve identificar quando um usuário procura autenticar a partir de um novo ASN;

3.79.4. Deve alertar quando um usuário procura se autenticar a partir de um país incomum pela primeira vez;

3.79.5. Deve alertar quando um usuário procura se autenticar em um país diferente;

3.79.6. Deve alertar uma anomalia quando um usuário procura se autenticar em vários países em um curto período de tempo, o que seria impossível;

3.79.7. Deve alertar quando uma conta de dispositivo e não uma conta de usuário tenta autenticar;

3.79.8. Deve alertar quando uma conta de serviço e não uma conta de usuário tenta autenticar;

3.79.9. Deve alertar quando um usuário tenta se autenticar de forma suspeita após não ter feito isso em um período de tempo;

3.79.10. Deve alertar quando um usuário tentar se autenticar com um sistema operacional novo ou anormal.

### 3.80. Capacidade de Detecção baseada em dados de nuvem

3.80.1. A solução deve ter a capacidade de ingerir dados da AWS, Azure e GCP;

3.80.2. A solução deve ter a capacidade de ingerir dados em nuvem, logs de tráfego, logs de auditoria integrando-se a uma solução CSPM (Cloud Security Posture Management);

3.80.3. Deve detectar quando uma identidade de nuvem que normalmente se conecta de um país ou conjunto de países se conecta de um país diferente pela primeira vez;

3.80.4. Deve detectar quando a configuração de uma trilha de log foi modificada;

3.80.5. Deve detectar quando um grupo do CloudWatch foi excluído;

3.80.6. Deve detectar quando um fluxo do CloudWatch foi excluído;

3.80.7. Deve detectar quando o gravador de configuração da AWS é interrompido para um recurso específico;

3.80.8. Deve detectar quando uma instância, em execução ou interrompida, é exportada para um bucket S3 externo;

3.80.9. Deve detectar quando um ou mais logs de fluxo são excluídos;

3.80.10. Deve detectar quando um detector AWS Guard Duty é removido;

3.80.11. Deve detectar quando um grupo de recursos do IAM é excluído, afetando as permissões dos membros;

3.80.12. Deve detectar quando um cluster RDS é removido;

3.80.13. Deve identificar quando uma função de entidade confiável é modificada;

3.80.14. Deve detectar quando uma chamada de API do AWS Systems Manager é feita de alguma instância;

3.80.15. Deve detectar quando um recurso do AWS Config é excluído;

3.80.16. Deve detectar quando uma regra ACL é criada com um número específico;

3.80.17. Deve detectar quando uma regra ACL é removida;

3.80.18. Deve detectar quando um usuário da AWS é criado;

3.80.19. Deve detectar quando uma Web ACL é removida;

3.80.20. Deve detectar quando um grupo do IAM é criado;

3.80.21. Deve detectar quando uma identidade recuperou o conteúdo do valor criptografado de um segredo específico no Secret Manager;

3.80.22. Deve identificar quando uma função da AWS foi assumida por uma identidade;

3.80.23. Deve identificar quando uma identidade despejou vários segredos do projeto, consideravelmente mais do que o normal;

3.80.24. Deve identificar quando um cluster do Aurora (RDS) é interrompido;

3.80.25. Deve detectar quando o registro de uma trilha de nuvem foi interrompido, suspenso ou excluído;

3.80.26. Deve detectar quando um alarme do Cloud Watch foi removido;

3.80.27. Deve detectar quando uma identidade executa uma chamada de API de computação para executar comandos arbitrários;

3.80.28. Deve detectar quando uma identidade realizou várias ações que foram negadas, o que pode indicar que ela está sendo usada indevidamente;

3.80.29. Deve detectar quando a criptografia foi desabilitada em servidores que hospedam instâncias do EC2, tanto para dados em repouso quanto em trânsito;

3.80.30. Deve detectar quando os atributos de um instantâneo de uma máquina EC2 foram modificados;

3.80.31. Deve detectar quando uma identidade acessou um recurso de armazenamento usando um agente de usuário incomum de um IP externo;

3.80.32. Deve identificar quando uma identidade de nuvem fez o download de um objeto de um bucket pela primeira vez;

3.80.33. Deve detectar quando uma API de nuvem foi chamada de um novo país na organização;

3.80.34. Deve ter a capacidade de ingerir dados do Azure;

3.80.35. Deve detectar quando uma política de Firewall do Azure é removida;

3.80.36. Deve detectar quando uma conta de automação do Azure foi criada;

3.80.37. Deve detectar quando um Runbook de Automação do Azure é criado, modificado ou excluído;

3.80.38. Deve detectar quando um Webhook de Automação do Azure é criado;

3.80.39. Deve detectar quando o nível de acesso de um contêiner Blob é alterado;

3.80.40. Deve detectar quando uma regra de autorização do Hub de Eventos do Azure é criada ou modificada;

3.80.41. Deve detectar quando um hub de eventos do Azure foi excluído;

3.80.42. Deve detectar quando há modificações no Azure Key Vault;

3.80.43. Deve detectar quando os Observadores de Rede do Azure são removidos;

3.80.44. Deve detectar quando os Grupos de Recursos são excluídos no Azure;

3.80.45. Deve detectar quando uma nova chave de uma conta de armazenamento do Azure é gerada;

3.80.46. Deve detectar quando uma configuração de diagnóstico do Azure é removida;

3.80.47. Deve detectar quando um usuário do Azure é criado;

3.80.48. Deve detectar quando uma VM do Azure executa comandos do Powershell com privilégios do sistema;

3.80.49. Deve ter a capacidade de ingerir dados do GCP;

3.80.50. Deve detectar quando um projeto de nuvem teve atividade incomum em uma região anteriormente inativa;

3.80.51. Deve detectar quando uma regra de firewall do GCP é modificada;

3.80.52. Deve detectar quando uma regra de firewall VPN no GCP é criada ou excluída;

3.80.53. Deve detectar quando um papel personalizado do IAM do G

3.80.54. Deve detectar quando um papel do GCP IAM é removido;

3.80.55. Deve detectar quando uma chave de conta de serviço do GCP IAM é criada, excluída ou desativada;

3.80.56. Deve detectar quando uma conta de serviço do GCP IAM é criada, excluída ou desativada;

3.80.57. Deve detectar quando um bucket de registros no GCP foi excluído;

3.80.58. Deve detectar quando uma entidade de coletor de registro de HCP foi modificada ou excluída;

3.80.59. Deve detectar quando uma assinatura do GCP Pub/Sub ou Topic foi excluída;

3.80.60. Deve detectar quando uma configuração de um bucket de armazenamento do GCP é modificada;

3.80.61. Deve detectar quando um bucket de armazenamento do GCP é excluído;

3.80.62. Deve detectar quando as permissões de um bucket de armazenamento do GCP são alteradas;

3.80.63. Deve detectar quando uma rede VPC do GCP é removida;

3.80.64. Deve detectar quando uma rota de rede é criada ou excluída em uma VPC;

3.80.65. Deve detectar quando uma identidade executa uma sequência de eventos que busca enumerar informações do IAM;

3.80.66. Deve detectar quando um usuário do IAM foi adicionado a um grupo do IAM;

3.80.67. Deve detectar quando um dispositivo MFA foi removido ou desassociado de um usuário do IAM;

3.80.68. Deve detectar quando uma identidade interna executou uma operação em várias regiões, consideravelmente mais do que o normal;

3.80.69. Deve detectar quando uma API na nuvem foi executada com sucesso usando uma ferramenta de teste de penetração;

3.80.70. Deve detectar quando uma conta root foi usada para fazer login no console da AWS;

3.80.71. Deve detectar quando um bucket do S3 foi excluído;

3.80.72. Deve detectar quando uma API foi chamada de um nó Tor;

3.80.73. Deve detectar quando uma identidade baixa vários objetos de um bucket, consideravelmente mais do que o normal;

3.80.74. Deve detectar quando uma identidade executa operações usando o AWS Systems Manager pela primeira vez;

3.80.75. Deve detectar quando um comando incomum que pode estar relacionado a uma enumeração de reconhecimento do IAM foi executado por uma identidade que não é um usuário;

3.80.76. Deve detectar quando uma identidade de nuvem executou pela primeira vez uma operação do IAM;

3.80.77. Deve detectar quando uma identidade de nuvem executou uma operação de gerenciamento de certificados pela primeira vez;

3.80.78. Deve detectar uma identidade na nuvem que realizou uma operação de gerenciamento de certificados pela primeira vez;

3.80.79. Deve detectar quando uma identidade de nuvem executou pela primeira vez uma operação de gerenciamento de segredos.

## 3.81. SERVIÇO DE GESTÃO DE VULNERABILIDADES

### 3.81.1. CARACTERÍSTICAS GERAIS

3.81.1.1. Deve ser ofertado pacotes de até 150 ativos.

3.81.1.2. Deve ser entregue como um serviço Software-as-a-Service (SaaS) em uma nuvem proprietária do fabricante para todos os seus serviços e aplicativos exigidos neste documento. Serviços fornecidos por nuvens de terceiros não são aceitos.

3.81.1.3. A gestão de todos os módulos considerados neste termo deve ser feita através de uma console única.

3.81.1.4. A solução deverá possuir no mínimo, duas das seguintes certificações de privacidade e segurança:

3.81.1.4.1. EU-U.S. Privacy Shield Framework;

3.81.1.4.2. Swiss-U.S. Privacy Shield Framework;

3.81.1.4.3. Cloud Security Alliance (CSA) STAR.

3.81.1.5. Todos os serviços da plataforma devem estar disponíveis sob o mesmo padrão de qualidade de serviço 24x7x365 e garantir 99% de disponibilidade.

3.81.1.6. O ofertante deve oferecer manutenção e atualização constante da plataforma durante todo o período de vigência do contrato de serviço.

3.81.1.7. As atualizações de serviço devem ser transparentes para o administrador da solução, sem afetar nenhum dos dados armazenados serviços fornecidos.

3.81.1.8. Todas as comunicações entre componentes, transferência de dados e sincronização da solução devem ser criptografadas de ponta a ponta, fazendo uso de no mínimo TLS 1.2, certificados assinados com RSA 2048 bits e algoritmo de assinatura SHA256.

3.81.1.9. A solução deve permitir criação de usuários distintos.

3.81.1.10. Deve permitir separação de funções e permissões na console.

3.81.1.11. Deve permitir integração através de SSO com, pelo menos, Okta e Azure Active Directory.

3.81.1.12. A console deve ser acessível a partir de, pelo menos, um dos navegadores comerciais dentre Google Chrome, Microsoft Edge e Firefox.

### 3.81.2. AGENTES

3.81.2.1. A solução proposta deve oferecer um agente de baixo impacto nos sistemas operacionais onde está instalado e no consumo de largura de banda que utilizará na rede.

3.81.2.2. A solução deve ser instalada em servidores, estações de trabalho, e máquinas virtuais, suportando sua implantação em rede local, em rede doméstica e na nuvem.

3.81.2.3. A solução deve oferecer suporte para sua implantação em pelo menos os seguintes sistemas operacionais:

3.81.2.4. Windows 7/Windows Server 2003 SP2 e posterior (x86, x64).

3.81.2.5. Red Hat Enterprise Linux/CentOS 6.5+, 7.x (x64), 8.x (x64).

3.81.2.6. Ubuntu 14, 16, 18, 19, 20 (x64).

3.81.2.7. Oracle Enterprise Linux 8, Oracle Enterprise Linux (OEL) 7 até 7.5, Oracle Enterprise Linux (OEL) 6.

3.81.2.8. Amazon Linux 2, Amazon Linux 2018.03, Amazon Linux 2017.09, Amazon Linux 2017.03.

3.81.2.9. SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 11.

3.81.2.10. FreeBSD 13.0, 12.2.

3.81.2.11. AIX 7.1 e 6.1.

3.81.2.12. Solaris 10 e 11.

3.81.2.13. O agente da solução deve se atualizar automaticamente e gerir as suas atualizações automaticamente.

3.81.2.14. A solução deve suportar plataformas de nuvem AWS, GCP, Azure.

3.81.2.15. A solução deve ser capaz de coletar informações sobre o inventário de ativos.

3.81.2.16. As funcionalidades de gestão de ativos, gestão de vulnerabilidade e detecção de patches devem ser fornecidas pelo mesmo agente de gerenciamento, não serão aceitas soluções com múltiplos agentes.

3.81.2.17. A solução deve prover nativamente um dispositivo capaz de concentrar requisições dos agentes para encaminhamento a console de gerenciamento de forma a evitar a conexão direta de agentes com a plataforma.

3.81.2.18. O agente de gerenciamento deve suportar o uso de proxy.

3.81.2.19. Deve ser possível definir o intervalo de comunicação entre o agente e a console de gerenciamento.

3.81.2.20. Deve ser possível limitar o consumo de CPU e memória do agente.

3.81.2.21. Deve permitir a definição de um período global de inatividade dos agentes.

### 3.81.3. SCANNERS

3.81.3.1. A solução deve permitir o uso de scanners capazes de identificar vulnerabilidades através de varreduras em ranges de IP definidos pelo administrador.

3.81.3.2. Não deverá haver restrições para instalação de scanners virtuais no ambiente.

3.81.3.3. Deve ser permitido o uso de scanners externos, sem necessidade de instalação, em nuvem própria do fabricante para varreduras de ativos publicados na internet.

3.81.3.4. Os scanners virtuais devem suportar pelo menos um dos hypervisors abaixo:

3.81.3.5. Hyper-V.

3.81.3.6. VMWare.

3.81.3.7. Os Scanners devem suportar a varredura de ambientes em nuvem para pelo menos os seguintes provedores:

3.81.3.8. Azure.

3.81.3.9. AWS.

3.81.3.10. Google Cloud Platform.

3.81.3.11. Oracle.

3.81.3.12. Os scanners devem reportar vulnerabilidades para console em nuvem, permitindo uma visão consolidada de vulnerabilidades.

3.81.3.13. Deve ser permitido o agendamento de varreduras para máquinas que possuam uma determinada versão de banco de dados em execução.

3.81.3.14. Deve ser permitido a varredura sob demanda para um ou mais ativos de rede.

3.81.3.15. O mesmo scanner deve ser capaz de varrer por falhas de conformidade e também por vulnerabilidades.

3.81.3.16. O scanner deverá consolidar vulnerabilidades encontradas em um ativo que possua agente instalado.

3.81.3.17. A solução deve permitir a configuração do tipo de varredura a ser realizada, permitindo pelo menos definir as seguintes configurações ao defini-la:

3.81.3.18. Configuração de quantidades de portas TCP/UDP a serem validadas.

3.81.3.19. Consumo de largura de banda e recursos (alto, médio, baixo).

3.81.3.20. Digitalize para dispositivos que não suportam ping traceroute.

3.81.3.21. Detecção de balanceadores de carga.

3.81.3.22. Configuração de força bruta para usar em senhas.

3.81.3.23. Uso de um cabeçalho HTTP personalizado.

3.81.3.24. Ignorar pacotes.

3.81.3.25. Instalação de agente temporário para validação de registro local.

### 3.81.4. CATEGORIZAÇÃO E INVENTÁRIO DE ATIVOS

3.81.4.1. A solução proposta deve permitir a coleta de informações detalhadas sobre o ativo gerenciado, deve detalhar pelo menos os seguintes dados para cada ativo:

3.81.4.2. Serviços em execução.

3.81.4.3. Software instalado.

3.81.4.4. Usuários.

3.81.4.5. Portas abertas.

3.81.4.6. Nome do host.

3.81.4.7. FQDN.

3.81.4.8. IP v4 / v6.

3.81.4.9. Endereço MAC.

3.81.4.10. Processador.

3.81.4.11. Memória.

3.81.4.12. Volumes de disco.

3.81.4.13. BIOS.

3.81.4.14. A solução deve classificar automaticamente os ativos por famílias de tecnologia, tipo de dispositivo, tipo

3.81.4.14. A solução deve classificar automaticamente os ativos por famílias de tecnologia, tipo de dispositivo, tipo de plataforma e fabricante.

3.81.4.15. A solução deve normalizar automaticamente os nomes dos fabricantes de HW e SW com seus dados relevantes, como o nome dos aplicativos e versões, para facilitar sua posterior busca na solução.

3.81.4.16. A solução deve possuir a habilidade de etiquetagem (Tags) de ativos para facilitar a identificação, devendo permitir a geração de Tags, pelo menos, usando os seguintes parâmetros:

3.81.4.17. Palavras-chave.

3.81.4.18. Endereço IP e intervalos de IP.

3.81.4.19. Segmento de rede.

3.81.4.20. Portas abertas.

3.81.4.21. Informações de inventário considerando, no mínimo:

3.81.4.22. Sistema operacional.

3.81.4.23. Presença ou ausência de determinado software instalado ou serviço em execução.

3.81.4.24. Última localização geográfica detectada incluindo cidade e país.

3.81.4.25. Groovy Scriptlet.

3.81.4.26. Regex.

3.81.4.27. A solução deve permitir agrupamento manual a critério do administrador da solução.

3.81.4.28. A solução deve permitir atribuir criticidade ao ativo para priorizá-lo durante o processo de gerenciamento.

3.81.4.29. Deve permitir criação de Dashboards personalizados que sejam capazes de trazer as seguintes informações sobre os ativos:

3.81.4.30. Categorias de softwares instalados nos ativos.

3.81.4.31. Hosts que executam máquinas virtuais.

3.81.4.32. Sistemas operacionais utilizados.

3.81.4.33. Serviços e portas TCP ou UDP abertas.

3.81.4.34. Softwares de segurança instalados.

3.81.4.35. Memória total utilizada.

3.81.4.36. Quantidade de processadores.

3.81.4.37. Quantidade de armazenamento disponível.

3.81.4.38. A solução deve permitir uma interface de busca de ativos que utilize uma sintaxe lógica baseada, no mínimo, nos critérios abaixo:

3.81.4.39. Fabricante de hardware.

3.81.4.40. Último usuário logado.

3.81.4.41. Categoria de software instalado.

3.81.4.42. A solução deve permitir a visualização da quantidade de máquinas com um determinado software instalado.

3.81.4.43. Deve permitir visualização de recursos em nuvem AWS ou Azure tais como VPCs, Virtual Networks, Security Groups, S3 buckets, RDS, SQL Server, sem necessidade de instalação de agentes ou varreduras de rede.

3.81.4.44. Deve permitir visibilidade a respeito de hosts que executam containers e containers em execução.

### 3.81.5. DETECÇÃO E RESPOSTA

3.81.5.1. A solução deve permitir descobrir, avaliar, priorizar e auxiliar na correção de vulnerabilidades/configurações em toda a infraestrutura de rede, incluindo estações de trabalho, servidores, dispositivos de rede, dispositivos de telecomunicações e dispositivos de segurança, hypervisors, máquinas virtuais, orquestradores de contêineres, contêineres e nuvens (Azure, GCP, AWS), proporcionando através de uma única interface para o administrador via um portal web para gerenciamento de todos os ativos, permitindo o gerenciamento centralizado de todos os componentes da solução a partir de um único ponto, sem a necessidade de incorrer em consoles ou componentes adicionais fora dele para a administração dos serviços oferecidos.

3.81.5.2. A solução deve ser oferecida na modalidade SaaS em nuvem própria do fabricante, sem necessidade de instalação de componentes locais para a gerência.

3.81.5.3. A solução deve ser licenciada por Asset (IP HOST) para ativos de infraestrutura.

3.81.5.4. A solução deve ser licenciada por URLs para varreduras de aplicação web.

3.81.5.5. A solução deve ser licenciada para 256 IP / HOST para varredura de vulnerabilidade, 256 HOST para Patch / Inventário varredura e scans.

### 3.81.6. GESTÃO DE VULNERABILIDADES

3.81.6.1. A solução deve permitir varreduras de vulnerabilidade com base em:

3.81.6.2. Sistemas Operacionais.

3.81.6.3. Serviços WEB.

3.81.6.4. Portas TCP e UDP.

3.81.6.5. Serviços.

3.81.6.6. Aplicações.

3.81.6.7. Bancos de dados.

3.81.6.8. Dispositivos de rede como switches, roteadores e balanceadores de carga.

3.81.6.9. No mínimo, a ferramenta deve abranger os seguintes sistemas operacionais, bancos de dados e aplicativos:

3.81.6.10. Microsoft Windows.

3.81.6.11. UNIX.

3.81.6.12. LINUX.

3.81.6.13. MacOS.

3.81.6.14. Mac OS X.

3.81.6.15. Cisco.

3.81.6.16. VMware.

3.81.6.17. Detectar e analisar vulnerabilidades nas principais versões de Bancos de Dados, pelo menos:

3.81.6.18. Microsoft SQL Server.

3.81.6.19. MySQL.

3.81.6.20. Oracle.

3.81.6.21. Sybase.

3.81.6.22. Detectar e analisar vulnerabilidades em plataformas WEB, pelo menos:

3.81.6.23. IIS.

3.81.6.24. Apache Tomcat.

3.81.6.25. Detectar e analisar vulnerabilidades em portas e serviços TCP e UDP.

3.81.6.26. Detectar vulnerabilidades em pelo menos os seguintes aplicativos ou plataformas:

3.81.6.27. Adobe.

3.81.6.28. Apple.

3.81.6.29. HP.

3.81.6.30. McAfee.

3.81.6.31. Microsoft (Office, IIS, Exchange).

3.81.6.32. Oracle.

3.81.6.33. Oracle Java.

3.81.6.34. VMware.

3.81.6.35. Permitir a descoberta de vulnerabilidades na rede, oferecendo as seguintes alternativas de varredura:

3.81.6.36. Varredura ativa de rede não autenticada.

3.81.6.37. Varredura ativa de rede autenticada.

3.81.6.38. Agente.

3.81.6.39. Varreduras externas.

3.81.6.40. O mecanismo de varredura deve ter uma taxa de precisão de detecção de vulnerabilidade de 99,99966% (seis sigma) durante os últimos 10 anos.

3.81.6.41. A base de conhecimento de vulnerabilidade deve ser atualizada semanalmente, garantindo a incorporação de pelo menos 20 CVEs a ela e deve ter pelo menos uma base de conhecimento de 35.000 CVEs relacionados, incluindo tecnologias legadas e atuais.

3.81.6.42. A solução deve oferecer suporte ao padrão da indústria para pontuação de vulnerabilidade do Common Vulnerability Scoring System (CVSS).

3.81.6.43. A solução deve oferecer suporte ao padrão da indústria para adicionar detecções personalizadas usando Open Vulnerability Assessment Language (OVAL).

3.81.6.44. A solução deve permitir vincular as vulnerabilidades detectadas e indicar sua relação com ameaças como Vírus, Trojan e Malware.

3.81.6.45. A solução deve ser capaz de indicar explorações disponíveis e códigos disponíveis para uma vulner

## 3.81.7. GESTÃO DE CONFIGURAÇÃO

3.81.7.1. A solução deve permitir a avaliação, o relatório e o relatório de problemas de configuração, com base nas referências do padrão da indústria do Centro de Segurança da Internet (CIS).

3.81.7.2. O fabricante deve ser oficialmente certificado pelo CIS para fornecer este nível de controles.

3.81.7.3. A solução deve oferecer avaliação de configuração com base no benchmark CIS padrão da indústria, cobrindo esta funcionalidade nas seguintes categorias:

3.81.7.4. Sistemas operacionais.

3.81.7.5. Software de servidor.

3.81.7.6. Provedores de nuvem.

3.81.7.7. Dispositivos de rede.

3.81.7.8. Software de desktop.

3.81.7.9. A solução deve suportar detecção de falhas de conformidade através de varreduras autenticadas ou através de agente instalado diretamente no ativo monitorado.

3.81.7.10. A solução deve permitir que os administradores recebam informações de conformidade de sistemas operacionais Windows e Linux, mesmo que não estejam conectados à rede corporativa.

3.81.7.11. A solução deve permitir a avaliação de certificados digitais (internos e externos) e configurações de TLS em busca de problemas e vulnerabilidades de certificados, resultando em diferentes graus de conformidade de acordo com os resultados da avaliação de seu emissor, prazo de validade, tipo de certificado, robustez do algoritmo e conjunto de criptografia usados.

### 3.81.8. DETECÇÃO E PRIORIZAÇÃO DE AMEAÇAS

3.81.8.1. A solução proposta deve permitir enviar alertas em tempo real sobre irregularidades na rede, identificar ameaças e monitorar mudanças inesperadas que ocorram na mesma.
3.81.8.2. A solução deve permitir enviar notificações para usuários específicos e grupos de usuários para o perfil de monitoramento perfis de monitoramento múltiplos.
3.81.8.3. A solução deve permitir a personalização do perfil de monitoramento associado a uma lista específica de critérios.
3.81.8.4. A solução deve permitir que os alertas sejam personalizados para uma ampla variedade de condições que afetam sistemas, certificados, vulnerabilidades, portas, serviços e

software. Cada regra deve permitir que seja configurada para detectar mudanças gerais comuns para se ajustar a circunstâncias muito específicas. 3.81.8.5. A solução deve permitir a atribuição de destinatários diferentes para cada alerta. 3.81.8.6. A solução deve enviar alertas de monitoramento sobre vulnerabilidades, configurações incorretas e outros parâmetros definidos pelo administrador da solução, incluindo:

3.81.8.7. Ativos com sistemas operacionais não aprovados.

3.81.8.8. Certificados expirados expirando.

3.81.8.9. Portas abertas.

3.81.8.10. Vulnerabilidades graves.

3.81.8.11. Tickets de correção abertos, resolvidos e fechados.

3.81.8.12. Software não aprovado.

3.81.8.13. A solução proposta deve fornecer fontes de inteligência de ameaças em tempo real e técnicas de aprendizado de máquina para fornecer controle de administrador sobre a evolução das ameaças relacionadas a vulnerabilidades encontradas nos ativos da organização e identificar quais corrigir primeiro.

3.81.8.14. A solução deve permitir consultas ad-hoc com múltiplas variáveis e critérios, como classe de ativo, tipo de vulnerabilidade, indicadores de ameaça em tempo real, etiqueta de ativo e sistema operacional, de modo que, por exemplo, seja possível pesquisar todas as vulnerabilidades que tenham uma alta classificação de gravidade, são fáceis de explorar e foram lançadas na semana passada.

3.81.8.15. A solução deve permitir que se faça uma correlação em tempo real das ameaças ativas contra as vulnerabilidades detectadas nos ativos corporativos.

3.81.8.16. A solução deve incluir indicadores de ameaças em tempo real que ajudam a avaliar e priorizar as vulnerabilidades detectadas, categorizados da seguinte forma:

3.81.8.17. Dia Zero: vulnerabilidades para as quais não há patch disponível e para as quais um ataque ativo foi observado.

3.81.8.18. Exploração pública: vulnerabilidades cujo mecanismo de exploração é conhecido, para o qual existe um código de exploração e está disponível publicamente.

3.81.8.19. Ataques ativos: vulnerabilidades que estão sendo atacadas ativamente.

3.81.8.20. Movimento lateral: vulnerabilidades que permitem ao invasor espalhar o ataque amplamente pela rede violada.

3.81.8.21. Fácil exploração: vulnerabilidades que podem ser facilmente exploradas, exigindo poucas habilidades e pouco conhecimento.

3.81.8.22. Perda de dados: vulnerabilidades cuja exploração causará perda massiva de dados.

3.81.8.23. Negação de serviço: vulnerabilidades cuja carga útil pode sobrecarregar impedir que sistemas comprometidos estejam permanentemente temporariamente disponíveis.

3.81.8.24. No Patch: vulnerabilidades para as quais não há solução do provedor.

3.81.8.25. Malware: vulnerabilidades associadas a infecções por malware.

3.81.8.26. Kit de exploração: vulnerabilidades para as quais um kit de exploração está disponível.

3.81.8.27. A solução deve atribuir uma pontuação a cada vulnerabilidade de forma contextual, quantificando o risco associado a esta vulnerabilidade.

3.81.8.28. Os fatores de risco devem considerar, pelo menos, três dos fatores abaixo:

3.81.8.29. Malwares associados.

3.81.8.30. Atores maliciosos associados.

3.81.8.31. Possibilidade de remediação.

3.81.8.32. A solução proposta deve fornecer um workflow de correção baseado em políticas de criação e atribuição, atribuindo tickets de acordo com as condições definidas pelo administrador da solução através de políticas ou manualmente.

3.81.8.33. A solução deve permitir a criação de tickets com status aberto, fechado, ignorado, com base nos seguintes critérios:

3.81.8.34. Host(s) a quem a regra se aplica.

3.81.8.35. Vulnerabilidade(s) a que a regra se aplica.

3.81.8.36. Usuário atribuído.

3.81.8.37. Data de criação - expiração.

3.81.8.38. Mudança de estado.

3.81.8.39. A solução deve permitir a criação de tickets de correção automaticamente a partir do resultado de uma varredura de vulnerabilidade - com base nas informações de um host específico e também manualmente por um administrador da solução.

### 3.81.9. GESTÃO DE PATCH

3.81.9.1. A solução proposta deve correlacionar vulnerabilidades e patches automaticamente para os hosts da sua organização.

3.81.9.2. A solução deve mapear automaticamente os patches com CVEs associados às vulnerabilidades detectadas.

3.81.9.3. Deve mostrar patches faltantes mesmo que não exista correlação com uma vulnerabilidade existente.

3.81.9.4. Deve mostrar patches faltantes para, no mínimo, as seguintes categorias:

3.81.9.5. Navegadores.

3.81.9.6. Ferramentas de compressão de arquivos.

3.81.9.7. Visualizadores de PDF.

3.81.9.8. Sistemas operacionais.

### 3.81.10. RELATÓRIOS E DASHBOARDS

3.81.10.1. A solução proposta deve permitir administração centralizada via interface gráfica WEB usando HTTPS.

3.81.10.2. A solução deve possibilitar o acesso à console de todos os componentes do serviço a partir de um único ponto.

3.81.10.3. A solução deve permitir a definição de diferentes perfis de usuários e funções para administração.

3.81.10.4. A solução deve fornecer controles de acesso de usuário hierárquicos e baseados em funções que permitem a delegação de responsabilidades para refletir a estrutura organizacional.

3.81.10.5. A solução deve permitir o acesso de um usuário autorizado de qualquer local.

3.81.10.6. A solução deve suportar integração com uma biblioteca API XML extensível.

3.81.10.7. A solução deve suportar autenticação de dois fatores para usuários e login.

3.81.10.8. A solução deve suportar configurações de segurança de senha.

3.81.10.9. A solução deve suportar personalizar a política de segurança para configurações de gerenciamento de senha, por:

3.81.10.10. Idade e expiração da senha.

3.81.10.11. Conta do usuário bloqueada após uma série de logins com falha.

3.81.10.12. Comprimento mínimo da senha.

3.81.10.13. Complexidade da senha, caracteres alfanuméricos e numéricos a serem usados.

3.81.10.14. Forçar mudança de senha no login inicial.

3.81.10.15. Notificação de senha expirada antes de vários dias.

3.81.10.16. A solução deve suportar a capacidade de restringir o acesso apenas à rede interna da empresa.

3.81.10.17. A solução deve suportar a capacidade de rastrear a atividade do usuário por nome da conta do usuário, data, ação e informações sobre a ação.

3.81.10.18. A solução deve suportar a capacidade de distribuir relatórios em PDF com segurança por meio de uma senha e um número restrito de downloads de relatórios por meio do link.

3.81.10.19. A solução deve suportar acesso por SSO (Single Sign-on) usando SAML 2.0.

3.81.10.20. A solução deve permitir o controle de alterações com trilhas de auditoria à prova de violação.

3.81.10.21. A solução proposta deve gerar relatórios por IPs, Grupo e Tags:

3.81.10.22. A solução deve permitir a geração de relatórios de qualquer IP - Host previamente verificado.

3.81.10.23. A solução deve permitir agendar relatórios diários, semanais, mensais e sob demanda.

3.81.10.24. A solução deve permitir o envio de notificações por email sempre que um relatório estiver disponível para o administrador da solução, usuários específicos e perfis diferentes criados na ferramenta.

3.81.10.25. A solução deve permitir pelo menos os seguintes tipos de relatórios:

3.81.10.26. Relatório de correção.

3.81.10.27. Relatório de vulnerabilidades altamente críticas.

3.81.10.28. Relatório Executivo.

3.81.10.29. Relatório de autenticação.

3.81.10.30. Relatório de conformidade normativa e regulatória.

3.81.10.31. Relatório de remediação.

3.81.10.32. A solução deve fornecer relatórios de correção por grupo de ativos, usuário e vulnerabilidade.

3.81.10.33. A solução deve permitir a criação de relatórios baseados em IPv4, endereços IPv6, nome do host, grupo de ativos e rótulos personalizados pelo administrador.

3.81.10.34. A solução deve permitir relatórios com cálculo de risco de segurança, permitindo um cálculo de risco global para todos os ativos incluídos no relatório.

3.81.10.35. A solução deve permitir relatórios que possibilitem o cálculo do risco do negócio, utilizando como base para o cálculo do risco de impacto ao negócio e do risco de segurança dos ativos incluídos no relatório.

3.81.10.36. A solução deve permitir relatar as descobertas com base no status das vulnerabilidades detectadas e seu status, conforme lista abaixo:

3.81.10.37. Novo.

3.81.10.38. Resolvido.

3.81.10.39. Reaberto.

3.81.10.40. Ativo.

3.81.10.41. A solução deve permitir relatórios que incluam vulnerabilidades com base na data de publicação.

3.81.10.42. A solução deve permitir incluir - excluir kernels Linux detectados na varredura de vulnerabilidade e que não estão em execução.

3.81.10.43. A solução deve permitir a exclusão de vulnerabilidades que você encontrará em uma porta ou serviço que não está em execução.

3.81.10.44. A solução deve permitir excluir vulnerabilidades que não são exploráveis devido à configuração do sistema/plataforma onde foi detectada.

3.81.10.45. A solução deve fornecer relatórios automatizados de tendências e diferenciais.

3.81.10.46. A solução deve fornecer várias opções de distribuição de relatórios, incluindo PDF criptografado.

3.81.10.47. A solução deve dar suporte à personalização do modelo de relatório conforme necessário.

3.81.10.48. A solução deve permitir a exportação de relatórios para os formatos HTML, MHT, PDF, DOC, CSV e XML.

3.81.10.49. A solução deve permitir que relatórios sejam apresentados em tabelas e gráficos com as ocorrências ocorridas, permitindo a customização detalhada de cada relatório.

3.81.10.50. A solução deve permitir em seus relatórios comparar o nível de conformidade entre políticas, tecnologias e ativos.

3.81.10.51. A solução deve possuir um painel (dashboard) que, por padrão, permite que você veja as tendências de vulnerabilidades por gravidade, plataforma, idade e status de remediação.

3.81.10.52. A solução deve permitir a customização dos painéis, fazendo uso de qualquer um dos dados disponíveis associados aos ativos varridos para selecionar diferentes tipos de gráficos, tabelas e visualizações sobre a priorização de vulnerabilidades.

3.81.10.53. A solução deve fornecer painéis executivos personalizáveis com uma visão unificada de todos os componentes da solução.

3.81.10.54. Deve ser possível criar dashboards que mostrem a pontuação de risco global de ativos e sua variação ao longo do tempo.

## 3.82. SERVIÇO DE GERENCIAMENTO DE ACESSO A CONTAS PRIVILEGIADAS COM COFRE DE SENHAS

3.82.1. CARACTERÍSTICA GERAL

3.82.1.1. Deve ser ofertado pacotes de no mínimo 150 dispositivos.

## 3.83. CARACTERÍSTICAS GERAIS DO COFRE DE SENHAS

3.83.1. Ser licenciado em subscrição, como SaaS ou On Premises, sem limite de usuários nominais ou eletrônicos (API).

3.83.2. A solução deve proteger contra a perda, roubo e gestão inadequada de credenciais através de regras de complexidade da senha que incluem comprimento da senha (quantidade de caracteres), frequência de troca da senha, especificação de caracteres permitidos ou proibidos na composição da senha e outras medidas.

3.83.3. Deve realizar o upload de arquivos como certificados, chaves de API, tokens, etc., para o cofre da solução de forma segura e auditada.

3.83.4. Deve realizar a funcionalidade de gerenciamento e armazenamento para sincronização de segredos para DevOps, com capacidade de se conectar e recuperar segredos do cofre de forma automática.

3.83.5. A solução deve ser capaz de controlar quais aplicativos podem ser usados por um operador na sessão, limitando o acesso a aplicativos especificados no sistema remoto, permitindo somente os executáveis listados (whitelist). Deve ser possível também optar por permitir ou negar o acesso à área de trabalho.

3.83.6. A solução deve gerenciar segredos para software e máquinas gerenciados, armazenados e recuperados programaticamente por meio de APIs e SDKs (isso inclui gerenciamento de segredos para aplicativos, técnicas de injeção de credenciais e impressão digital de aplicativos).

3.83.7. Deve ser capaz de se integrar e rotacionar credenciais para contas de administradores sem exigir o LAPS (Solução de Senhas de Administrador Local Microsoft).

3.83.8. Deve possuir integração com os sistemas operacionais a seguir com a utilização de APIs para a compatibilidade:

3.83.8.1. Microsoft Windows Server 2012 e superiores;

3.83.8.2. Red Hat Enterprise Linux Server 6.0 e superiores;

3.83.8.3. Oracle Enterprise Linux 7.2 e superiores;

3.83.8.4. Ubuntu Linux 2.6 e superiores;

3.83.8.5. CentOS Linux 6.1 e superiores;

3.83.8.6. Suse Linux;

3.83.8.7. Ambientes de virtualização VMWare ESXi 7.2 e superiores;

3.83.8.8. Sistemas gerenciadores de banco de dados Oracle, Microsoft SQL Server, MySQL, PostgreSQL e Teradata;

3.83.8.9. Ferramentas de busca e análise de dados ElasticSearch;

3.83.8.10. Equipamentos de rede e de segurança Huawei Technologies, Dell, CheckPoint, Cisco Systems, Extreme Networks, Broadcom e F5 Networks Big-IP, Fortinet;

3.83.8.11. Controladores de storage Huawei Technologies, PureStorage e Veritas NetBackup;

3.83.8.12. Aplicações Microsoft Windows, incluindo contas de serviço, tarefas agendadas e pools de conexão do IIS;

3.83.8.13. Aplicações Web, incluindo JBoss, Tomcat, Oracle Application Server, Apache e IIS;

3.83.8.14. Aplicações em nuvem, incluindo Microsoft Azure, Amazon AWS e Office 365.

3.83.9. A solução deve suportar o acesso a desktops, servidores e outros sistemas remotos autônomos, suportando os seguintes modos:

3.83.10. Acesso através de cliente de proxy local, que permite o acesso a sistemas Windows/Linux autônomos em uma rede, sem cliente pré-instalado;

3.83.11. Acesso a dispositivos de rede habilitados para SSH/telnet através de um cliente de proxy efetuando a conexão localmente;

3.83.12. Ser composto por cofre de senhas, elemento responsável pela geração, revogação, versionamento, armazenamento e controle das credenciais de acesso, e por gateway ou proxy de sessão, elemento responsável pelo provimento do acesso privilegiado, monitoramento e controle de sessão;

3.83.13. Ao acessar um ativo baseado em Linux, a injeção de credenciais deve suportar sua utilização em conjunto com o SUDO;

3.83.14. A fim de proteger contra erros comuns do usuário durante as sessões SSH, a solução deve suportar filtro de comandos, para bloquear alguns comandos e permitir que outros, em um esforço para evitar que o usuário inadvertidamente use um comando que pode causar resultados indesejáveis;

3.83.15. A solução deve suportar o uso de um certificado válido assinado por CA que valida seu novo endereço de acesso à ferramenta ou suportar o uso da autoridade certificadora grátis "Let's Encrypt" para obter um certificado;

3.83.16. Deve gerenciar o acesso à conta para Hypervisors, como Vsphere ou Hyper-V, iniciando uma sessão de aplicativo segura e injetando credenciais. Depois que as sessões são encerradas, as credenciais devem ser rotacionadas;

3.83.17. Ser implantado com os recursos mínimos e suficientes para o provimento do serviço, incluindo a criptografia do sistema operacional e do sistema de gerenciamento de banco de dados (hardening);

3.83.18. Incluir, caso necessário, o licenciamento necessário de Microsoft Remote Desktop Server, para acesso comum a servidores e/ou aplicativos (Remote App);

3.83.19. A solução deve ser capaz de realizar a integração de forma automatizada de contas e permissões aos seus recursos;

3.83.20. Realizar o gerenciamento de credenciais, em que credencial é qualquer senha, chave criptográfica ou token capaz de ser guardado de maneira segura, garantindo os seguintes aspectos:

3.83.20.1. Rotatividade de credenciais, permitindo a geração de senhas aleatórias para ativos e grupo de ativos;

3.83.20.2. Ser possível reverter para uma credencial anterior caso haja alguma incompatibilidade;

3.83.21. Revogação de credenciais sob demanda ou por meio de política definida;

3.83.22. Especificação do tipo de caracteres para a composição de senhas, incluindo caracteres alfabéticos maiúsculos, minúsculos, numéricos, especiais e símbolos, por ativos ou grupo de ativos;

3.83.23. Definição de tempo de validade de credenciais;

3.83.24. Criptografia de credenciais com protocolos padrões da indústria, incluindo AES 256;

3.83.25. Capacidade de reinicialização de serviços e dependências, no caso de mudança de uma credencial de serviço;

3.83.26. Segmentação de senhas, por autorização de múltiplos aprovadores;

3.83.27. Injeção automática de credenciais, de modo que a autenticação se realize sem que o usuário tenha conhecimento ou precise conhecer a senha;

3.83.28. Exportação da chave de criptografia ou da credencial equivalente do cofre de senhas, para uso em caso de recuperação de desastres ou de migração de solução;

3.83.29. Possuir funcionalidade de discovery, capaz de buscar e registrar novos ativos alvo, garantindo as seguintes condições:

3.83.29.1. Capacidade de realizar buscas no Active Directory e em blocos de endereços IP, podendo ser realizada por demanda, agendada e rotina periódica;

3.83.29.2. Capacidade de especificar o DN ao pesquisar usuários no servidor LDAP;

3.83.29.3. Levantamento de contas administrativas em cada ativo;

3.83.29.4. Levantamento de ativos e de suas respectivas identidades em grupos, de acordo com parâmetros previamente configurados;

3.83.29.5. Classificação automática de contas locais e de domínio;

3.83.29.6. Identificação de contas de serviços e de tarefas em ambientes Microsoft Windows;

3.83.29.7. Identificação de contas locais e que possuam chaves SSH em ambientes Unix/Linux;

3.83.30. A solução deve ser capaz de gerenciar contas em vários domínios do AD. As contas a serem gerenciadas devem incluir Conta de administrador padrão do domínio, contas locais no servidor/estação de trabalho, SQL Server Admin (SA) e contas privilegiadas do Azure AD;

3.83.31. Deve ter a capacidade de aplicar a segregação de funções, por exemplo, permitindo que os administradores do Windows vejam apenas as sessões do Windows.

3.83.32. Não conter restrição em relação ao quantitativo de contas que podem ser gerenciadas em um dispositivo licenciado.

## 3.84. CARACTERÍSTICAS GERAIS DO SERVIÇO DE ACESSO A CONTAS PRIVILIGEDIADAS

3.84.1. A solução deve ter a opção de ser disponibilizada no modelo SaaS;

3.84.2. A arquitetura, quando em SaaS, não deve requerer nenhuma abertura de porta, regra de firewall, VPN ou qualquer fluxo de dado no sentido entrante (inbound) apenas saliente (outbound);

3.84.3. A comunicação entre o ambiente local e a nuvem da solução deve ser criptografada, não permitindo a utilização de protocolos antigos, como TLS 1.0;

3.84.4. A retenção de dados de gravação de sessão deve ser, pelo menos, de 1 ano, sem custo adicional ou limite de utilização de espaço;

3.84.5. Quando em SaaS, atividades como início de sessão, descobrimento de ativos e rotação de senha não devem acontecer no ambiente SaaS;

3.84.6. A solução, quando em SaaS, deve possuir proxy de comunicação local, com capacidade de executar os processos descritos no item anterior em camada 2, sem que essas atividades aconteçam no servidor da aplicação na nuvem;

3.84.7. A disponibilidade do ambiente em cloud deve ser, pelo menos, de 99.9%, garantida pelo fabricante e/ou provedor da cloud;

3.84.8. A solução SaaS deve ter, pelo menos, a certificação SOC2 válida;

3.84.9. A solução caso on premises, deve ser disponibilizada como máquina virtual, compatível ao menos com VMware e Hyper-V;

3.84.10. A arquitetura on premises deve permitir modo de redundância ativo/passivo ou ativo/ativo;

3.84.11. Caso opte-se por ativo/ativo, a solução deve armazenar o banco de dados externamente ao servidor de aplicação e sessão, permitindo que a CONTRATANTE utilize sua estrutura de banco de dados e redundância;

3.84.12. A solução deve permitir o desmembramento das funções do produto em diversos nós, por exemplo: servidor de rotação de senhas, servidor de acessos, servidor de gerência de forma individual e apartada, permitindo o escalonamento da operação, sem custo adicional;

3.84.13. Ser capaz de monitorar sessões, gravar sessões, capturar telas, coletar, armazenar e indexar logs de teclas pressionadas em teclado (keystrokes) em acessos privilegiados, garantindo os seguintes requisitos:

3.84.13.1. Alerta ao usuário privilegiado que a sessão está sendo gravada;

3.84.13.2. Monitoramento por meio de gravação de vídeos, em formato padrão de execução da solução;

3.84.13.3. Monitoramento ao vivo, permitindo ao usuário supervisor, previamente configurado, realizar ações de lock/unlock, suspender e terminar a conexão;

3.84.13.4. Pesquisa forense de eventos de segurança em todas as sessões gravadas, incluindo comandos digitados, copiar e colar arquivos e execução de softwares;

3.84.14. As funcionalidades de gerenciamento e monitoramento de sessões devem impedir que os usuários executem determinadas ações durante uma sessão e ser capazes de executar ações automaticamente na detecção de eventos de sessão configurados nas políticas de acesso (Ex.: Suspender a sessão do usuário);

3.84.15. Deverá ter a capacidade de registrar sessões privilegiadas e armazená-las de forma segura em um repositório criptografado e inviolável. A gravação da sessão não deve afetar o desempenho do dispositivo de destino;

3.84.16. Controlar e monitorar sessões usando protocolos padrões e acesso remoto, incluindo RDP, HTTP/HTTPS e SSH;

3.84.17. Ser capaz de recuperar senhas guardadas na solução, em caso de inviabilidade de conexão por meio de sessão auditada, para acesso direto ao ativo;

3.84.18. Integrar-se com soluções de autenticação de duplo fator através do protocolo RADIUS, Single Sign-On via SAML ou OIDC e Time-Based One-Time Password (TOTP);

3.84.19. Garantir que os usuários da solução tenham visualização somente dos recursos que têm capacidade de requerer acesso;

3.84.20. Permitir o agrupamento lógico de sistemas alvo de modo a simplificar a configuração de políticas de acesso;

3.84.21. Deve possuir campos personalizados armazenados para contas/recursos privilegiados no sistema;

3.84.22. Tais personalizações podem ser usadas para rotular ativos e pode definir atributos para cada ativo em um grupo;

3.84.23. Possuir recurso que permita a integração de terceiros utilizando scripts, macros, comandos, chamadas executáveis e protocolos de rede, incluindo SSH, API REST e HTTP/HTTPS;

3.84.24. Deve automatizar a alocação de acesso entre administradores e suas contas pessoais de administrador;

3.84.25. Garantir requisitos de segurança na guarda de credenciais, incluindo criptografia no tráfego de informações, suportando, no mínimo, TLS 1.2;

3.84.26. Gerenciar senhas privilegiadas de aplicações, de modo a evitar que sejam senhas estáticas em códigos-fonte (hardcoded), garantindo os seguintes aspectos:

3.84.26.1. Solicitação de credenciais via REST sob demanda ao invés de credenciais estáticas;

3.84.26.2. Atualização automática de contas no banco de dados de senhas;

3.84.26.3. Inscrição automática de sistemas alvo sem aguardar por atualizações dinâmicas;

3.84.26.4. Configurações de segurança que garantam o acesso apenas por aplicações permitidas, suportando no mínimo o endereço de origem das requisições, nome de usuário, autenticação por certificados e/ou caminho da aplicação.

3.84.27. Permitir a criação de fluxos customizáveis de aprovação de acesso privilegiado, garantindo os seguintes aspectos:

3.84.27.1. Configuração de acessos pré-aprovados;

3.84.27.2. Interface para solicitar e aprovar acessos, com exposição do motivo;

3.84.27.3. Notificação em casos de acessos não aprovados para solicitantes.

3.84.28. Exigir aprovação antes do início de uma sessão, suportando no mínimo uma notificação por e-mail de aprovação enviada aos destinatários designados sempre que uma tentativa de sessão com qualquer ativo, solicitando que o usuário insira um motivo da solicitação, a hora e a duração da solicitação.

3.84.29. Prover interface Web para administração da solução, permitindo a autenticação por meio de usuário e senha local, Active Directory, LDAP e métodos de multifatores (MFA);

3.84.30. Capacidade de rastrear atividades de usuários privilegiados e acesso à identidade do usuário original para garantir que os requisitos de responsabilidade sejam atendidos;

3.84.31. Possuir mecanismo de backup e restore de todos os dados e configuração da solução, incluindo recurso de exportação para um servidor remoto, de maneira automática ou agendada;

3.84.32. Prover relatórios de auditoria que disponibilizem informações das interações dos usuários, tais como atividades de login, adição e remoção de senhas privilegiadas, endereço IP de máquina de origem e do destino alvo, atividades administrativas de delegação e revogação de acesso e eventos agendados. Os relatórios devem ser filtrados por período, tipo de operação, sistema e usuários;

3.84.33. Deve possuir suporte a diferentes idiomas, possuindo, mas não se limitando a:

3.84.33.1. Inglês

3.84.33.2. Português

3.84.33.3. Espanhol

3.84.34. Prover relatórios de conformidade que disponibilizem operações, incluindo lista de sistemas gerenciados, eventos de alteração de senha, auditoria de contas e alertas de segurança;

3.84.35. Deve ser possível gerar relatórios em HTML, CSV e PDF;

3.84.36. Deve ter a capacidade de exportar relatórios para diferentes formatos de arquivo;

3.84.37. Para certos grupos de usuários, a solução deve permitir forçar o encerramento da sessão, forçando a sessão a se desconectar no horário final agendado. Nesse caso, o usuário deve receber notificações antes de ser desconectado;

3.84.38. Incluir o fornecimento de módulo de acesso remoto seguro, na modalidade SaaS ou on premises para pelo menos 2 usuários simultâneos;

3.84.39. O módulo de acesso seguro deverá ser licenciado como subscrição, em SaaS ou On Premises;

3.84.40. O módulo de acesso seguro, quando em SaaS, deve ser baseado em "Tenant" localizado no Brasil;

3.84.41. Suportar o acesso externo à rede sem qualquer necessidade de utilização de VPN ou método similar de acesso;

3.84.42. Permitir o acesso remoto, no mínimo, aos seguintes sistemas operacionais:

3.84.43. Microsoft, Desktop e Servidores;

3.84.44. Linux Red Hat Enterprise e similares;

3.84.45. Utilizar protocolos de comunicação fazendo uso de criptografia TLS 1.2 ou superior;

3.84.46. Suportar o funcionamento em redes que não estão conectadas diretamente à internet e a redes seguras;

3.84.47. Suportar o acesso sem necessidade de permissão prévia para o acesso a desktops e servidores;

3.84.48. Possibilitar o acesso a dispositivos de rede via SSH, como roteadores e switches;

3.84.49. Disponibilizar aos usuários console de acesso Web para a solução, sem a necessidade de instalação de plug-ins ou agentes;

3.84.50. Suportar provedores externos de identidades para autenticação, incluindo, no mínimo, servidores LDAP, Active Directory, RADIUS e Kerberos, bem como atribuir privilégios com base na hierarquia e nas configurações de grupo já especificadas nos respectivos servidores;

3.84.51. Integrar-se com soluções de autenticação de duplo fator através de protocolo RADIUS, Single Sign-On via SAML ou OIDC e Time-Based One-Time Password (TOTP);

3.84.52. Suportar o uso de um certificado assinado por uma autoridade certificadora válida;

3.84.53. Permitir o agendamento para liberação do acesso remoto, incluindo notificação por e-mail aos destinatários designados;

3.84.54. Permitir forçar o encerramento da sessão remota pelo supervisor, com notificação ao cliente;

3.84.55. Prover monitoramento ao vivo e gravação da sessão, com registro completo das atividades executadas durante a sessão pelos usuários;

3.84.56. Limitar o acesso a aplicativos especificados no sistema remoto, incluindo o acesso à área de trabalho remota;

3.84.57. Suportar filtro de comandos durante as sessões SSH, visando evitar que o usuário inadvertidamente use um comando que pode causar danos ao servidor acessado;

3.84.58. Suportar a injeção automática de credenciais em sistemas Windows, permitindo que os usuários autentiquem ou elevem privilégios sem revelar credenciais, bem como a ação de "executar como";

3.84.59. Suportar a injeção automática de credenciais em sistemas Unix/Linux, permitindo que os usuários autentiquem ou elevem privilégios sem revelar credenciais, bem como a utilização em conjunto com o sudo;

3.84.60. Suportar o acesso com os seguintes modos:

3.84.60.1. Através de clientes instalados;

3.84.60.2. Através de agente de proxy local, que permite o acesso a sistemas autônomos em uma rede, sem cliente pré-instalado;

3.84.60.3. Acesso via agente de proxy local, que permite o acesso a sistemas em uma rede remota que não tenha uma conexão de internet nativa;

3.84.60.4. Suportar Remote Desktop Protocol (RDP), permitindo que os usuários colaborem em sessões auditadas e gravadas;

3.84.60.5. Prover acesso a dispositivos de rede habilitados para SSH através de um cliente de proxy efetuando a conexão localmente;

3.84.60.6. Prover acesso a páginas Web a partir de agente de proxy local, onde os usuários receberão apenas uma conexão a uma página Web local em uma sessão auditada e gravada;

3.84.61. Permitir o monitoramento em tempo real das sessões de acesso feitas a ativos publicados na ferramenta;

3.84.62. Permitir a configuração de tempos limites para sessões ociosas, em que seja possível definir o tempo máximo para que um usuário inativo seja desconectado automaticamente;

3.84.63. Permitir que os usuários transfiram arquivos da máquina em que está conectado para o sistema remoto, através da console da solução e sem necessidade de uso de ferramentas de terceiros;

3.84.64. Permitir que os usuários compartilhem sessões de acesso com outros usuários do sistema, permitindo que os administradores colaborem em uma mesma sessão. Esta colaboração deve ser possível com usuários internos e externos através de convite;

3.84.65. Oferecer aos usuários conectados a capacidade de ver informações do sistema sem que seja necessário ter acesso à console do ativo;

3.84.66. Oferecer aos usuários a capacidade de executar tarefas do sistema fora do compartilhamento de tela, como por exemplo reiniciar um serviço em servidores com sistema operacional Windows;

3.84.67. Oferecer a opção de prover acesso à linha de comandos dos servidores sem a necessidade de compartilhamento de tela, permitindo aos administradores a execução de comandos remotos via conexões lentas de internet;

3.84.68. A solução deve poder operar de forma autônoma, sem a necessidade de integração com soluções de cofre de senhas para armazenar os ativos, segredos e credenciais, caso seja necessário;

3.84.69. A solução deve contar com funcionalidade de página de auto registro para prestadores de serviço, para que eles mesmos possam solicitar a criação de seus usuários sem a necessidade de intervenção manual de um administrador;

3.84.70. A solução deve possibilitar a instalação de um cliente na máquina do utilizador, sem a necessidade de utilizar um navegador para acessar o dispositivo alvo;

3.84.71. A solução deve permitir realizar o encaminhamento de portas localmente na máquina do usuário final (Ex.: O usuário deve poder criar um encaminhamento localhost:8080 -> 192.168.0.10:443);

3.84.72. A solução deve suportar instalação de agente no dispositivo alvo, para que a máquina possa ser acessada em qualquer localidade, sem a necessidade de instalação de servidor de proxy local;

3.84.73. A solução deve permitir o cadastramento de scripts personalizados, que podem ser disponibilizados para os usuários através de lista de permissão;

3.84.74. A solução deve permitir que prestadores de serviço possam cadastrar ou descadastrar ativos;

3.84.75. Deve ser possível personalizar a URL de acesso, bem como o certificado digital que será utilizado na aplicação em SaaS ou on premises;

3.84.76. A solução deve possuir ferramentas de anotação, permitindo que o usuário faça anotações na tela durante a sessão sem utilizar recursos do sistema operacional alvo;

3.84.77. A solução deve permitir a parametrização da ação quando a sessão é finalizada (Ex.: Ao finalizar a sessão a máquina alvo é bloqueada, o usuário é bloqueado, ou nada ocorre);

3.84.78. A solução deve permitir que as políticas de acesso sejam exportadas e importadas, em formato criptografado;

3.84.79. A solução deve permitir que indicadores de performance, como utilização de CPU, Disco e UPTIME, sejam coletados pelo agente de conexão remota instalado;

3.84.80. A solução deve possuir funcionalidade de "Wake on Lan" para os dispositivos gerenciados.

## 3.85. SERVIÇO DE TESTE DE PENETRAÇÃO

### 3.85.1. DA EXECUÇÃO DOS SERVIÇOS

3.85.1.1. Deve ser ofertado um pacote de até 3000 horas de Serviço.

3.85.1.2. Os serviços deverão ser executados somente após a emissão de Ordem de Execução de Serviço (OES), com a obrigatória autorização pelo CONTRATANTE.

3.85.1.3. O prazo máximo para início das atividades será de até 10 (dez) dias úteis após a abertura da OES.

3.85.1.4. Os serviços serão prestados na forma REMOTA.

3.85.1.5. Os testes e avaliações não poderão impactar o pleno funcionamento dos recursos testados, nem ativo porventura relacionado, sem explícita e prévia autorização e monitoração pela equipe técnica responsável do CONTRATANTE.

3.85.1.6. O CONTRATANTE poderá solicitar a mudança de metodologia e/ou do cronograma, inclusive podendo requerer a execução dos testes em finais de semana, feriados ou fora do

horário comercial quando houver algum risco na execução do teste de invasão (PENTEST) que possa comprometer, em qualquer grau, o funcionamento de seus sistemas, ativos ou processos.

3.85.1.7. A formalização de solicitação do teste de invasão (PENTEST) será feita em OES específica.

3.85.1.8. O Cronograma de Atividades utilizado para cumprimento da OES, será:

| | | |
|---|---|---|
| Prazo padrão: | Dia: 1 a 10 | Dia: 11 a 25 |
| Atividades: | Fase de Planejamento e preparação | Realização do reconhecimento, análise de vulnerabilidades, exploração, entrega do relatório de teste de invasão (PENTEST) e reunião de encerramento. |
| Responsabilidade | CONJUNTA | CONTRATADA |

3.85.1.9. Este Cronograma de Atividades servirá como referência, podendo ser ajustado entre as partes na fase de planejamento e preparação, devendo ser adotado o prazo máximo de 25 (vinte e cinco) dias corridos para o início do teste de invasão (PENTEST).

3.85.1.10. O CONTRATANTE irá realizar a avaliação do relatório de teste de invasão (PENTEST) bem como aplicar as correções que entender passíveis de serem executadas para posterior solicitação de reteste, a ser encaminhada para CONTRATADA no prazo máximo de 6 (seis) meses a contar do Recebimento Definitivo da OES.

3.85.1.11. O serviço de reteste entende-se como a garantia de serviço.

3.85.1.12. Do teste de invasão (PENTEST), é obrigatório quando forem realizadas ações corretivas pelo CONTRATANTE, devendo ser concluído no prazo máximo de 30 (trinta) dias corridos a contar do recebimento da solicitação encaminhada pelo CONTRATANTE.

3.85.1.13. Quando solicitado o reteste, a CONTRATADA deverá:

3.85.1.14. Apresentar relatório de reteste seguindo os mesmos requisitos do relatório de teste de invasão (PENTEST).

## 3.85.2. ESPECIFICAÇÃO TÉCNICA DO SERVIÇO DE PENTEST.

3.85.2.1.1. Os Serviços de Teste de invasão (PENTEST) têm como objetivo principal identificar, mapear e documentar possíveis ameaças e vulnerabilidades nos ativos e infraestrutura tecnológica, processos, sistemas e aplicações WEB. Esses serviços envolvem, necessariamente, o uso de técnicas e ferramentas específicas para tentar obter acesso não autorizado e privilegiado aos ativos e informações, bem como a indicação de soluções para a correção das ameaças e vulnerabilidades encontradas.

3.85.2.1.2. Os termos “Teste de invasão (PENTEST)", "Pentest”, "teste de penetração", "teste de intrusão" e "teste de invasão" são considerados sinônimos.

3.85.2.1.3. Os pentests poderão ser realizados em qualquer dos serviços, ativos, infraestrutura, rede e sistemas de TI publicados na internet em qualquer porta lógica e que pertençam ao domínio e faixas de IP tecnológicos.

3.85.2.1.4. Os pentests poderão ser realizados por meio de VPN concedida à CONTRATADA ou a partir da Internet.

3.85.2.1.5. Os sistemas, serviços e ativos de TI tecnológicos da CONTRATADA a serem submetidos aos testes serão definidos em OES.

3.85.2.1.6. Durante os testes, sem autorização prévia e monitoração pela equipe técnica responsável do CONTRATANTE, não poderão ser executados quaisquer variações dos seguintes ataques:

3.85.2.1.7. Ataques de negação de serviços (Denial of Service – DoS – e Distributed Denial of Service - DDoS) e flooding.

3.85.2.1.8. Engenharia social, por exemplo, phishing, vishing, pharming, personificação, roubo de identidade e outros.

3.85.2.1.9. Ataques que possam causar danos físicos, por exemplo, arrombamentos, danos às fechaduras eletrônicas, ativação de sistemas de alarme.

3.85.2.1.10. Ataques que envolvam vetores de infecção, tais como ransomware, vírus, worms, trojan, rootkits e outros.

3.85.2.1.11. Todos os testes deverão ser supervisionados pelo CONTRATANTE.

3.85.2.1.12. A equipe da CONTRATADA deve interagir e funcionar de maneira integrada com a equipe do CONTRATANTE. A equipe da CONTRATADA deve compartilhar seu conhecimento no sentido de indicar soluções para possíveis vulnerabilidades encontradas para que, por meio da atuação conjunta com o CONTRATANTE, aumente-se a efetividade da proteção do ambiente.

3.85.2.1.13. Para a realização dos serviços de Teste de invasão (PENTEST) deverão ser observadas as orientações e técnicas emanadas pelos padrões internacionais, além de outros apresentados pela CONTRATADA, caso haja em seu portfólio normativos que comprovadamente complementem:

3.85.2.1.14.1. OSSTMM 3 (The Open-Source Security Testing Methodology Manual).

3.85.2.1.14.2. ISSAF/PTF (Information Systems Security Assessment Framework).

3.85.2.1.14.3. NIST Special Publication 800115 (Technical Guide to Information Security Testing and Assessment).

3.85.2.1.14.4. NIST Special Publication 80042 (Guideline on Network Security Testing).

3.85.2.1.14.5. OWASP TESTING GUIDE 3.0 The Open Web Application Security Project.

3.85.2.1.15. As ferramentas utilizadas nas atividades de Teste de invasão (PENTEST) são de responsabilidade da CONTRATADA, não devendo ser instaladas no ambiente tecnológico do CONTRATANTE.

3.85.2.1.16. Quaisquer problemas que venham a comprometer o bom andamento dos serviços devem ser imediatamente comunicados ao CONTRATANTE.

3.85.2.1.17. O serviço de Teste de invasão (PENTEST), realizado em infraestrutura, sistemas e aplicações WEB, deverá obedecer às seguintes fases, pelo menos:

3.85.2.1.18. Planejamento e preparação.

3.85.2.1.19. Reconhecimento e análise de vulnerabilidades.

3.85.2.1.20. Exploração.

3.85.2.1.21. Relatório de Teste de invasão (PENTEST) (Técnico e Executivo/Gerencial).

3.85.2.1.22. Reunião de encerramento, para apresentação do relatório de recomendações e descrição das atividades executadas durante o teste.

3.85.2.1.23. Reteste, quando realizadas correções por parte do CONTRATANTE.

3.85.2.1.24. Relatório de reteste, quando necessário o reteste.

3.85.2.1.25. Planejamento e preparação:

3.85.2.1.26. Todas as premissas, processos, atividades descritas e aprovadas na OES, inclusive os cronogramas, serão detalhados e apresentados na fase de planejamento e preparação.

3.85.2.1.27. Informações sobre o ambiente corporativo, utilizando-se das seguintes técnicas (podendo ser utilizadas ambas, conforme definição do escopo a critério do CONTRATANTE):

3.85.2.1.27.1. Técnica da caixa-preta (pouco ou nenhum conhecimento sobre o ambiente a ser avaliado, o ambiente deverá ser descoberto pelo especialista).

3.85.2.1.27.2. Técnica da caixa branca (o avaliador tem acesso irrestrito a qualquer informação que possa ser relevante ao teste).

3.85.2.1.27.3. Técnica da caixa cinza ou híbrida (conhecimento limitado sobre o alvo).

## 3.85.3. RECONHECIMENTO E ANÁLISE DE VULNERABILIDADES.

3.85.3.1.1. Poderão ser utilizadas ferramentas de análise de vulnerabilidades e técnicas manuais de análise de vulnerabilidade. As ferramentas deverão ser apresentadas para ciência e aprovação antes de sua efetiva utilização, assim como a metodologia para análise manual de vulnerabilidades.

3.85.3.1.2. Deverão ser atendidos os seguintes quesitos e estarem devidamente apresentados no Relatório de Teste de invasão (PENTEST):

3.85.3.1.3. Coleta passiva, onde deverá ser utilizada, no mínimo, as seguintes técnicas:

3.85.3.1.3.1. Whois e nslookup (consultas DNS).

3.85.3.1.3.2. Sites de busca.

3.85.3.1.3.3. Listas de discussão.

3.85.3.1.3.4. Blogs de colaboradores.

3.85.3.1.3.5. Informações livres.

3.85.3.1.3.6. Packet sniffing “passive eavesdropping”.

3.85.3.1.3.7. Captura de banner.

3.85.3.1.4. Coleta ativa, onde deverá ser utilizada, no mínimo, as seguintes técnicas:

3.85.3.1.4.1. Port scanning (Mapeamento de rede).

3.85.3.1.4.2. Varredura de vulnerabilidade.

3.85.3.1.5. Varredura de vulnerabilidade que deverá verificar/identificar, entre outros:

3.85.3.1.5.1. Hosts ativos na rede.

3.85.3.1.5.2. Portas e serviços em execução.

3.85.3.1.5.3. Serviços ativos e vulneráveis nos hosts.

3.85.3.1.5.4. Sistemas operacionais.

3.85.3.1.5.5. Vulnerabilidades associadas com sistemas operacionais e aplicações descobertas.

3.85.3.1.5.6. Configurações feitas nos hosts sem observância de boas práticas em segurança computacional.

3.85.3.1.5.7. Identificação de rotas e estimativa de impacto, caso estas sejam modificadas/desconfiguradas.

3.85.3.1.5.8. Identificação de vetores de ataque e cenários para exploração.

3.85.3.1.5.9. Vulnerabilidades Detectadas (CVE).

3.85.3.1.5.10. Vulnerabilidades de Alto Risco.

3.85.3.1.5.11. Vulnerabilidades de Médio Risco.

3.85.3.1.5.12. Vulnerabilidades de Baixo Risco.

3.85.3.1.5.13. Network Vulnerability Tests (NVT).

3.85.3.1.5.14. Dos serviços e aplicações web:

3.85.3.1.5.15. Uso indevido de sistema de arquivos e arquivos temporários.

3.85.3.1.5.16. Evasão de informação por configurações default de tratamento de erros.

3.85.3.1.5.17. Tratamento indevido de entrada.

3.85.3.1.5.18. Problemas relacionados à má configuração dos serviços.

3.85.3.1.5.19. Gerenciamento inseguro de sessões web.

## 3.85.4. EXPLORAÇÃO

3.85.4.1. Quaisquer atividades com suspeita de comprometimento de algum ambiente ou ativo deverão ser imediatamente reportadas, antes de sua execução, haja vista a necessidade de manter a disponibilidade dos ambientes e serviços ativos.

3.85.4.2. Inicialmente, deverão ser efetuados procedimentos automatizados e manuais de reconhecimento, varredura e descoberta, de forma a coletar informação que forneçam subsídios para uma eventual exploração das vulnerabilidades encontradas. Se encontradas vulnerabilidades exploráveis, deverão ser reportadas ao CONTRATANTE, sem a devida exploração, de forma a avaliar a extensão prática de um eventual ataque bem-sucedido.

3.85.4.3. A CONTRATADA, durante a execução do trabalho, deve comprovar a realização de Teste de invasão (PENTEST)/testes de intrusão manuais, por meio de gravação de tela e logs, entregues em mídia digital no encerramento de cada OES.

3.85.4.4. A CONTRATADA deverá avaliar o perímetro e proteção do domínio do CONTRATANTE que pode incluir qualquer ativo que compõem a infraestrutura de um sistema/aplicação WEB e que pertençam ao domínio e faixas de IP tecnológicos da Prefeitura de Pindamonhangaba, bem como páginas ou telas com campos de formulários ou web services.

3.85.4.5. Deverão ser alvos destas etapas os elementos ativos que ofereçam serviços à internet e intranet, desde que possam representar ameaças aos serviços ou à rede interna e zonas desmilitarizadas (DMZ), em caso de efetivo comprometimento. Esses alvos podem ser, por exemplo, firewalls, proxies, switches, roteadores, desktops, servidores (Windows ou Linux), físicos ou virtuais, appliances, storage, entre outros.

3.85.4.6. Deverão ser avaliados também os serviços críticos de comunicação, topologia, arquitetura, políticas, configurações e outros elementos integrantes de esquemas de proteção, aplicações WEB, além da infraestrutura de roteamento.

3.85.4.7. Deverão ser incluídos no relatório todos os endereços IPs analisados e os respectivos serviços encontrados com seus fingerprints.

3.85.4.8. Caso haja identificação, registro e ataque a uma vulnerabilidade considerada grave pela CONTRATADA, esta deverá notificar o CONTRATANTE imediatamente.

3.85.4.9. A CONTRATADA não deverá alterar a integridade das informações, ou seja, não deve alterar as informações de servidores e sistemas que possam comprometer os serviços prestados pelo CONTRATANTE.

3.85.4.10. A CONTRATADA deverá manter sigilo absoluto sobre as possíveis vulnerabilidades encontradas.

3.85.4.11. Deverá realizar testes de vulnerabilidades em endereços IP's, URL's, aplicações ou outro ativo definido do ambiente computacional, composto por servidores, banco de dados, ativos de rede, ativos de segurança e outros equipamentos relacionados ao Teste de invasão (PENTEST).

3.85.4.12. Poderão ser aplicados os seguintes tipos de ataques, entre outros:

3.85.4.12.1. Violações do protocolo HTTP.

3.85.4.12.2. SQL Injection.

3.85.4.12.3. LDAP Injection.

3.85.4.12.4. Cookie Tampering e cookie/session poisoning.

3.85.4.12.5. Cross-Site Scripting (XSS).

3.85.4.12.6. Directory Transversal.

3.85.4.12.7. Buffer Overflow.

3.85.4.12.8. OS Command Execution.

3.85.4.12.9. Command Injection.

3.85.4.12.10. Remote Code Inclusion.

3.85.4.12.11. Server Side Includes (SSI) Injection.

3.85.4.12.12. File disclosure.

3.85.4.12.13. Information Leak.

3.85.4.12.14. Zero-day attacks.

3.85.4.12.15. Dos (Denial of Service).

3.85.4.12.16. DDos (Distributed Denial of Service).

3.85.4.12.17. Contra protocolo TCP.

3.85.4.12.18. Ataques contra a aplicação.

3.85.4.12.19. Procura de serviços privilegiados desprotegidos e existência de backdoors.

3.85.4.12.20. Race conditions.

3.85.4.12.21. Spoofing.

3.85.4.12.22. Testes remotos de quebra de senhas via dicionário e/ou força bruta, inclusive a serviços de diretórios de usuários LDAP e Banco de Dados.

3.85.4.12.23. Acesso a documentações e a equipamentos.

3.85.4.12.24. Identificação de compartilhamentos de pasta e níveis de permissão através de varredura no parque computacional.

3.85.4.13. Para ataques em nível da aplicação:

3.85.4.13.1. Buffer Overflow.

3.85.4.13.2. Problemas com o SNMP.

3.85.4.13.3. Vírus, worms, cavalos de Tróia e demais malwares.

3.85.4.14. Associadas a serviços Web servers, FTP servers, Mail servers, DNS servers, SSH Servers, servidores de Domínio Microsoft, servidores de arquivos, impressão, filtro de conteúdo.

3.85.4.15. Associadas a aplicações web expostas ao público interno.

3.85.4.16. Injeção de Código:

3.85.4.17. Ataques XSS (Cross-site Scripting).

3.85.4.18. Comprometimento do acesso remoto.

3.85.4.19. Manutenção de acesso.

3.85.4.20. Encobrimento de rastros da invasão.

3.85.4.21. Para o "Teste de invasão (PENTEST)" direcionados, especificamente, aos serviços prestados via WEB, tanto Intranet quanto Internet, deverão ser observados e aplicados os seguintes testes baseados na publicação OWASP TESTING GUIDE 3.0 (The Open Web Application Security Project):

3.85.4.22. Para testes de coleta de informações, aplicar padrão: OWASPIG001, OWASPIG002, OWASPIG003, OWASPIG004, OWASPIG005 e OWASPIG006.

3.85.4.23. Para testes de gerenciamento de configuração, aplicar padrão: OWASPCM001, OWASPCM002, OWASPCM003, OWASPCM004, OWASPCM005, OWASPCM006, OWASPCM007, OWASPCM008.

3.85.4.24. Para testes de autenticação, aplicar padrão: OWASPAT001, OWASPAT002, OWASPAT003, OWASPAT004, OWASPAT005, OWASPAT006, OWASPAT007, OWASPAT008, OWASPAT009 e OWASPAT010.

3.85.4.25. Para testes de gerenciamento de sessão, aplicar padrão: OWASPSM001, OWASPSM002, OWASPSM003,

3.85.4.26. OWASPSM004, OWASPSM005.

3.85.4.27. Para testes de autorização, aplicar padrão: OWASPAZ001, OWASPAZ002 e OWASPAZ003.

3.85.4.28. Para testes de negócio lógico, aplicar padrão: OWASPBL001.

3.85.4.29. Para testes de validação de dados, aplicar padrão:

3.85.4.29.1. OWASPDV001; OWASPDV002, OWASPDV003, OWASPDV004, OWASPDV005,

3.85.4.29.2. OWASPDV006, OWASPDV007, OWASPDV008, OWASPDV009, OWASPDV010, OWASPDV011, OWASPDV012, OWASPDV013, OWASPDV014, OWASPDV015 e OWASPDV016.

3.85.4.30. Para testes de negação de serviços, aplicar padrão: OWASPDS001, OWASPDS002, OWASPDS003, OWASPDS004, OWASPDS005, OWASPDS006, OWASPDS007 e OWASPDS008.

3.85.4.31. Para testes de serviços web, aplicar padrão: OWASPWS001, OWASPWS002, OWASPWS003, OWASPWS004, OWASPWS005, OWASPWS006 e OWASPWS007.

3.85.4.32. Observa-se que o resultado de cada teste deverá vir acompanhado de relatórios contendo:

3.85.4.33. Referência-base (Whitepaper).

3.85.4.34. Ameaças encontradas.

3.85.4.35. Riscos levantados ao ambiente computacional.

3.85.4.36. Contramedidas para mitigar as ameaças encontradas.

3.85.4.37. Para fins de estimativa de esforço, a CONTRATADA deverá considerar até 5 aplicações WEB a serem analisadas, podendo ser formulários ou web services e até 25 ativos que compõem a infraestrutura. A lista com estes itens deverá constar na Ordem de Execução de Serviço emitida pelo CONTRATANTE.

3.85.4.38. O objetivo será o de verificar o comportamento dos sistemas em relação às expectativas de confidencialidade das informações trocadas nas mensagens, resistência às tentativas de burlar o controle de acesso e boa utilização de algoritmos criptográficos, entre outros.

3.85.4.39. O diagnóstico de segurança das aplicações deverá incluir, mas não se limitar a:

3.85.4.39.1. Avaliação do grau de confiança da aplicação nos dados oriundos do usuário e possibilidade de operações de bypass.

3.85.4.39.2. Resistência das aplicações quanto a ataques do tipo “Man in the Middle”.

3.85.4.39.3. Teste de injeção de comandos.

3.85.4.39.4. Níveis de risco oriundos de configurações de permissões de acesso na aplicação.

3.85.4.39.5. Possibilidade de imposição de identidade por exploração de falhas de autorização, caso existam.

3.85.4.39.6. Análise do comportamento da aplicação para averiguar se, a partir de falhas de segurança na aplicação, é possível interagir com recursos do sistema operacional e banco de dados que suporta a mesma.

3.85.4.39.7. Análise do comportamento da aplicação em relação aos sistemas operacionais que as abrigam, procurando identificar falhas que possam ser exploradas por usuários com acesso aos sistemas, mas não autenticados pelas aplicações.

3.85.4.40. Outros tipos de testes técnicos de segurança da aplicação, a depender das suas características intrínsecas.

3.85.4.41. Encontradas vulnerabilidades exploráveis, deverão ser reportadas ao CONTRATANTE. Caso haja autorização expressa, poderão ser efetuados testes de intrusão em profundidade, de forma a determinar até onde e em que condições as eventuais vulnerabilidades poderiam ser utilizadas por um eventual atacante, e a extensão prática de um ataque. Deverão ser sugeridas políticas, configurações ou ações que venham a conter ou detectar ataques de mesma natureza.

### 3.85.5. RELATÓRIO DE ETHICAL HACKING.

3.85.5.1. Deverá ser elaborado e entregue ao CONTRATANTE após a fase de exploração, o relatório "RELATÓRIO de ETHICAL HACKING" para cada OES que será realizada, contemplando no mínimo as seguintes informações:

3.85.5.1.1. Objetivos, premissas e escopo do teste, datas e horas dos testes, metodologia de análise de vulnerabilidades, descrição das ações realizadas, metodologias, vulnerabilidades encontradas, categorização e severidade das vulnerabilidades, possíveis problemas aplicáveis, recomendações e controles de segurança necessários para correção das vulnerabilidades, apresentação das evidências apuradas, fontes de pesquisa, referências e ferramentas utilizadas, informações acessadas e demais evidências de sucesso em caso de invasão.

3.85.5.1.2. Detalhes da infraestrutura descoberta, alvo do Teste de invasão (PENTEST).

3.85.5.2. Descrição dos cenários/ambiente e análises

3.85.5.3. Descrição dos equipamentos, recursos demandados para as atividades e técnicas utilizadas.

3.85.5.4. Tipos de ataque.

3.85.5.5. Pontos positivos e negativos encontrados na infraestrutura de segurança/aplicação do CONTRATANTE.

3.85.5.6. Prazos (janelas de tempo para execução dos testes).

3.85.5.7. Pontos de contato da CONTRATADA (responsáveis para tratamento de questões abordadas nos testes).

3.85.5.8. Tipos de testes realizados pelos especialistas em segurança da informação.

3.85.5.9. Confirmação ou refutação da existência de vulnerabilidades.

3.85.5.10. Documentação sobre o caminho utilizado para exploração, avaliação do impacto e prova da existência da vulnerabilidade.

3.85.5.11. Obtenção de acesso e possível escalada de privilégios.

3.85.5.12. Detalhamento da metodologia do ataque.

3.85.5.13. Resultados efetivos da análise/testes/ataques.

3.85.5.14. Recomendações para sanar riscos e vulnerabilidades.

3.85.5.15. Diretrizes para o System Hardening dos servidores, serviços de rede, elementos ativos e aplicações testados.

3.85.5.16. A reunião de encerramento de cada OES, para apresentação do relatório de recomendações e descrição das atividades executadas durante o teste, poderá ser realizada por vídeo ou nas dependências do CONTRATANTE, a critério do CONTRATANTE.

3.85.5.17. A reunião será conduzida pela CONTRATADA que deverá apresentar de forma detalhada todo o conteúdo do “Relatório de Teste de invasão (PENTEST)” e sanar todas as dúvidas do corpo técnico do CONTRATANTE.

3.85.5.18. Após a entrega do "RELATÓRIO DE TESTE DE INVASÃO (PENTEST)", o CONTRATANTE analisará o documento para aplicar as recomendações, remediar os riscos ou mesmo assumi-los.

3.85.5.19. Relatório de Reteste:

3.85.5.20. Após essa análise e aplicadas medidas de remediação, o CONTRATANTE poderá solicitar à CONTRATADA que refaça os testes para aferição dos resultados com emissão de novo relatório.

3.85.5.21. Atividades de Apoio:

3.85.5.21.1. Para auxílio das atividades poderão, a critério do CONTRATANTE, serem solicitados à CONTRATADA os seguintes documentos de apoio:

3.85.5.21.2. PLANO DE TRABALHO com o detalhamento do escopo dos testes e cronograma de execução.

3.85.5.21.3. APRESENTAÇÃO INICIAL das ações a serem aplicadas pela CONTRATADA.

3.85.5.21.4. RELATÓRIOS DE ACOMPANHAMENTO SEMANAIS do plano de trabalho.

### 3.85.6. COMPROVAÇÃO DE CONHECIMENTO TÉCNICO DA CONTRATADA.

3.85.6.1. Apenas para esse serviço serão exigidas as seguintes certificações específicas relacionadas ao serviço de PENTEST:

3.85.6.2. A CONTRATADA deverá comprovar ter em seu corpo técnico no mínimo duas ou três das seguintes certificações:

3.85.6.2.1. CompTIA Pentest+

3.85.6.2.2. DCPT

3.85.6.2.3. OSWP

3.85.6.2.4. OSCP

3.85.6.2.5. CEH Master

## 3.86. DOS SERVIÇOS GERENCIADOS DE INFRAESTRUTURA.

3.86.1. A CONTRATADA deverá disponibilizar uma equipe de pessoas tecnicamente capacitadas, as quais serão responsáveis pela operação total do ambiente;

3.86.1.1. Será responsabilidade da CONTRATADA arcar com todos os custos, referentes aos recursos, sem nenhum ônus financeiro, ou vínculo empregatício para a CONTRATANTE.

3.86.1.2. Deverá disponibilizar um recurso responsável por coordenar as operações, que será o ponto focal para todas as necessidades da CONTRATANTE.

3.86.1.3. A função deste recurso é facilitar a comunicação entre a CONTRATANTE e as demais equipes da CONTRATADA (Redes, Servidores, Segurança, etc.), de forma a garantir o cumprimento de todos os níveis de serviço, e priorizar as atividades de acordo com as necessidades da CONTRATANTE.

3.86.1.4. O atendimento pela equipe deverá ser feito preferencialmente de maneira REMOTA, sendo requisitado o atendimento presencial somente quando necessária intervenção física nos equipamentos.

3.86.1.5. A equipe ficará disponível em regime 9x5 (nove horas por dia, cinco dias por semana), no horário das 9:00 às 18:00.

3.86.1.6. A equipe deve ser formada de, no mínimo, 01 profissional de cada uma das seguintes áreas de atuação:

3.86.1.6.1. Gerente/coordenador de operações;

3.86.1.6.2. Redes (Switches, balanceador de carga);

3.86.1.6.3. Virtualização;

3.86.1.6.4. Sistemas operacionais (Windows);

3.86.1.6.5. Armazenamento;

3.86.1.6.6. Backup;

3.86.1.7. Responsabilidades e atividades da equipe.

3.86.1.8. Realizar os serviços de operação da solução.

3.86.1.9. Realizar a criação e alteração de máquinas virtuais.

3.86.1.10. Realizar a criação e alteração de políticas de snapshots e backups.

3.86.1.11. Realizar a criação de volumes e aggregates.

3.86.1.12. Realizar a criação e gerenciamento de VLANS.

3.86.1.13. Realizar a configuração de políticas de QoS para priorizar o tráfego de rede.

3.86.1.14. Realizar a configuração de funcionalidades de segurança, como ACLs (Access Control Lists), autenticação 802.1X, e port security.

3.86.1.15. Realizar a configuração de protocolos de redundância, como STP (Spanning Tree Protocol) e RSTP (Rapid Spanning Tree Protocol).

3.86.1.16. Auxiliar a CONTRATANTE no planejamento e implementação de configurações avançadas.

3.86.1.17. Realizar os serviços de monitoramento.

3.86.1.18. Realizar o atendimento de tickets/chamados abertos pela CONTRATADA no sistema da CONTRATANTE.

3.86.1.19. Realizar operações de mudança (Gerência de Mudanças) aprovadas pela CONTRATANTE.

3.86.1.20. Realizar a interface entre as necessidades da CONTRATANTE e os profissionais da CONTRATADA que são responsáveis por executar as atividades.

## 3.87. SERVIÇO DE TRANSBORDO DE CÓPIAS DE SEGURANÇA – TIPO FRIO

3.87.1.1.1. O provedor que integra a solução deve possuir, no mínimo, as certificações: ABNT NBR ISO/IEC 27001:2013; ABNT NBR ISO/IEC 27017:2016 ou CSA STAR Certification LEVEL TWO ou superior; e ISO/IEC 27018:2019, com validade vigente na data de assinatura do contrato, referentes à infraestrutura de datacenter no Brasil onde os serviços em nuvem estarão hospedados.

3.87.1.1.2. As certificações ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27017:2016 poderão ser apresentadas nas suas versões originais em inglês: ISO/IEC 27001:2013 e ISO/IEC 27017:2015.

3.87.1.1.3. A CONTRATADA comprometer-se-á a preservar os dados da CONTRATANTE contra acessos indevidos e abster-se-á de replicar ou realizar cópias de segurança (backups) destes dados fora do território brasileiro, devendo informar imediatamente e formalmente à CONTRATANTE qualquer tentativa, inclusive por meios judiciais, de acesso por parte de outra nação a estes dados.

3.87.1.1.4. A solução deve permitir autenticação de usuário para controlar o acesso aos dados, como mecanismos de controle de acesso, como políticas de permissões e Listas de Controle de Acesso (ACLs) para conceder seletivamente permissões para usuários e grupos de usuários.

3.87.1.1.5. A solução deve permitir realizar de forma segura o upload/download de dados, utilizando o protocolo S3.

3.87.1.1.6. A solução deverá prover mecanismo de acesso protegido aos dados, por meio de chave de criptografia, garantindo que apenas aplicações e usuários autorizados tenham acesso.

3.87.1.1.7. A solução deverá permitir a criptografia automática de dados e objetos armazenados usando AES (Advanced Encryption Standard) de, no mínimo, 256 bits ou outro algoritmo com força de chave equivalente ou superior, neste último caso desde que aprovado pela CONTRATANTE.

3.87.1.1.8. A solução deverá possibilitar comunicação criptografada e protegida para transferência de dados.

3.87.1.1.9. Proteger os dados em trânsito entre um aplicativo e a nuvem pública usando a criptografia TLS.

3.87.1.1.10. Deve suportar que os dados sejam criptografados automaticamente quando gravados no Armazenamento usando a Criptografia do Serviço de Armazenamento.

3.87.1.1.11. O armazenamento deve ser altamente escalável e atender às necessidades de desempenho e armazenamento de dados dos aplicativos atuais.

3.87.1.1.12. A solução de armazenamento em nuvem deverá:

3.87.1.1.12.1. Ser geograficamente replicada em no mínimo três data centers;

3.87.1.1.12.2. Os data centers deverão estar localizados no território nacional;

3.87.1.1.12.3. Fornecer disponibilidade aos dados em até 48 (quarenta e oito) horas, caso solicitado;

3.87.1.1.12.4. Possuir período mínimo de retenção de 180 (cento e oitenta) dias.

3.87.1.1.13. Os dados no armazenamento devem ser acessíveis de qualquer lugar no mundo por HTTP ou HTTPS. O fabricante deve fornecer SDKs para o Armazenamento em várias linguagens - .NET, Java, Node.js, Python, PHP, Ruby, Go e outras - assim como uma API REST. O Armazenamento deve oferecer suporte para scripts PowerShell.

3.87.1.1.14. A solução de armazenamento em nuvem deverá suportar os seguintes casos de uso:

3.87.1.1.15. Fornecimento de imagens ou de documentos diretamente a um navegador.

3.87.1.1.16. Armazenamento de objetos para acesso distribuído.

3.87.1.1.17. Armazenamento de dados de backup e restauração, recuperação de desastres e arquivamento.

3.87.1.1.18. Armazenamento de dados para análise por um serviço local ou hospedado.

## 3.88. SERVIÇO DE CONVERSÃO DE APLICAÇÕES PARA TECNOLOGIAS DE CONTAINER

3.88.1.1. Planejamento de migração de máquina virtual para tecnologia de container;

3.88.1.2. Avaliação das aplicações em execução na máquina virtual com o intuito de viabilizar a migração para container;

3.88.1.3. Construção de imagem de container do tipo dockerfile, docker-compose e/ou YAML;

3.88.1.4. Configuração de escalabilidade automática de containers, isto é, “autoscaling”;

3.88.1.5. Configuração do servidor de host da tecnologia de container;

3.88.1.6. Configuração e adição de novos hosts ao cluster de container;

3.88.1.7. Instalação e configuração de drivers para acesso a volumes físicos do tipo bloco;

3.88.1.8. Instalação e configuração de drivers para acesso a volumes físicos do disco rede;

3.88.1.9. Configuração de serviço de monitoramento com indicadores e métricas para os hosts da tecnologia de container;

3.88.1.10. Implementação e configuração de serviço de gerenciamento de identidade;

3.88.1.11. Serviço de monitoramento através da implementação de métricas e indicadores dos serviços de containers para geração de alertas;

3.88.1.12. Implementação de ferramenta para orquestração de containers;

3.88.1.13. Implementação de ferramenta para gerenciamento, monitoramento e operação de containers;

3.88.1.14. Serviços de conversão de aplicações sem e com controle de estado;

3.88.1.15. Os serviços deverão ser realizados em horário comercial.

## 3.89. SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO

### 3.89.1. CARACTERÍSTICAS GERAIS DA INSTALAÇÃO E CONFIGURAÇÃO

3.89.1.1. Entende-se por serviços de instalação e configuração como sendo as atividades de planejamento e execução de configurações físicas e lógicas de componentes de hardware e software.

3.89.1.2. A CONTRATADA deverá apresentar um plano de Implementação, contemplando todas as suas fases, marcos e entregáveis.

3.89.1.3. Os serviços de instalação da Solução serão supervisionados pela CONTRATANTE, através de funcionário(s) designado(s) para esta atividade, preliminarmente ao início da execução, durante a execução até o término da execução da instalação.

3.89.1.4. A CONTRATADA deverá indicar 01 (um) Gerente de Projeto, funcionário ou contratado da empresa, que será o líder e responsável pela entrega dos serviços de implementação das soluções contratadas, de modo a garantir a qualidade dos resultados e o atendimento aos requisitos e prazos estipulados neste edital.

3.89.1.5. O Gerente de Projeto indicado deverá possuir certificação PMP – Project Management Professional do PMI – Project Management Institute.

3.89.1.6. Os documentos de certificação deverão ser apresentados, por ocasião da assinatura do contrato, na versão original ou por qualquer processo de cópia autenticada em cartório.

3.89.1.7. O Gerente de Projeto deverá ter experiência comprovada mediante apresentação de documento(s) contemplando a descrição geral dos serviços prestados, datas iniciais e finais de execução dos serviços com breve avaliação dos resultados, quanto ao cumprimento dos objetivos do projeto, com destaque para o gerenciamento do mesmo.

3.89.1.8. A CONTRATADA deverá apresentar declaração emitida pela mesma de que possui ou possuirá, durante a execução contratual, profissionais qualificados detentores de certificados técnicos na solução proposta responsáveis pela execução dos serviços. Estes profissionais deverão ser apresentados antes do início da execução dos serviços.

3.89.1.9. A instalação da solução deverá ser realizada por uma empresa, equipe ou profissional qualificado na solução ofertada.

3.89.1.10. A instalação da solução não poderá ocorrer por empresa, equipe ou profissional diferente da CONTRATADA neste processo.

3.89.1.11. É responsabilidade da CONTRATADA a execução dos serviços de implementação das soluções contratadas.

3.89.1.12. Todos os serviços de instalação e configuração deverão ser executados de forma presencial, por especialista(s) técnico(s) certificado(s) nos componentes pelos fabricantes.

3.89.1.13. A solução contempla a aquisição de hardware, software e suporte.

3.89.1.14. Entende-se como instalação:

3.89.1.14.1. O recebimento de todos os equipamentos nas localidades;

3.89.1.14.2. Conferência física dos itens;

3.89.1.14.3. Instalação física de hardware e software adquiridos, energização e ativação dos equipamentos adquiridos pelo CONTRATANTE;

3.89.1.14.4. Instalação física em rack padrão 19” disponibilizado pela CONTRATADA;

3.89.1.15. A CONTRATADA executará os serviços sem qualquer interferência no funcionamento regular das atividades normalmente realizadas pelo CONTRATANTE, garantindo a continuidade dos serviços, ou seja, não poderá haver interrupção não programada do serviço de dados atual para a entrada do novo serviço. Desta forma, executará serviços em finais de semana, feriados e horário noturno, sempre que houver necessidade para atendimento das condições expostas pelo CONTRATANTE nesta especificação.

3.89.1.16. Todas as configurações serão realizadas em conformidade com a recomendação do fabricante do equipamento e os requisitos fornecidos pelo CONTRATANTE para o ambiente em questão.

3.89.1.17. Ao término da instalação e configuração poderá ser considerada uma sessão de perguntas e respostas no local, com o objetivo de abordar os pontos principais e de funcionalidades chave dos produtos instalados.

3.89.1.18. A CONTRATADA deverá seguir sua metodologia própria no processo de instalação.

3.89.1.19. A CONTRATADA deverá responsabilizar-se pela conformidade e qualidade dos serviços e bens, bem como de cada material, matéria-prima ou componente individualmente considerado, mesmo que não sejam de sua fabricação, garantindo seu perfeito desempenho.

## 3.90. SERVIÇO DE CONVERSÃO DE APLICAÇÕES PARA TECNOLOGIAS DE CONTAINER

### 3.90.1. CARACTERÍSTICAS DA MIGRAÇÃO

3.90.1.1. Os serviços de migração da solução serão supervisionados pelo CONTRATANTE, através de funcionário (os) designado (s) para esta atividade, preliminarmente ao início da execução, durante a execução até o término da execução da migração;

3.90.1.2. Todas os servidores virtuais e aplicações a serem migradas devem fazer parte da matriz de compatibilidade da solução ofertada.

3.90.1.3. O serviço de migração deverá contemplar a migração de até 15 (quinze) máquinas virtuais;

3.90.1.4. A migração da solução deverá ser realizada por uma empresa, equipe ou profissional qualificado na solução de armazenamento inteligente ofertada.

3.90.1. 5. A migração não poderá ser realizada por empresa, equipe ou profissional diferente da CONTRATADA neste processo.

3.90.1.6. Deverá ser migrado todos os dados existentes do CONTRATANTE incluindo as transformações e ações necessárias nos dados para a correta adequação na solução de armazenamento, processamento e orquestração.

3.90.1.7. A migração dos dados deverá ser iniciada em até 15 (quinze) dias corridos após a fase de instalação da solução integrada de armazenamento, processamento e orquestração.

3.90.1.8. A CONTRATADA deverá seguir sua metodologia própria ou acordada com o CONTRATANTE no processo de migração.

## 3.91. CARACTERÍSTICAS DE TREINAMENTO

### 3.91.1. CARACTERÍSTICAS GERAIS DOS TREINAMENTOS

3.91.1.2. Os treinamentos deverão ser realizados nas seguintes condições:

3.91.1.3. Nas dependências de um centro autorizado, ou nas dependências da CONTRATANTE ou online via conferência com os participantes assegurado acesso ao novo ambiente para execução de tarefas hands-on, em data e hora acordada entre as partes;

3.91.1.4. Ministrado no período mínimo de 24 (vinte e quatro) horas;

3.91.1.5. O treinamento deverá ser feito para até 04 (quatro) participantes;

3.91.1.6. O treinamento deverá ser na modalidade de repasse de conhecimento, considerando o escopo mínimo de:

3.91.1.7. Visão geral dos componentes, instalação, configuração, operação e gerenciamento da solução;

3.91.1.8. A CONTRATADA deverá prover treinamento na modalidade de repasse de conhecimento com uma visão geral de todos os produtos e serviços oferecidos na solução.

3.91.1.9. A ementa citada no subitem anterior deverá ser aceita pela CONTRATADA, podendo ela também sugerir inclusão ou exclusão de algum tópico;

3.91.1.10. Havendo necessidade deverão ser utilizados equipamentos similares aos adquiridos, sendo possível poderão ser utilizados os próprios equipamentos adquiridos;

3.91.1.11. Deverá ser realizado por profissionais que tenham qualificação técnica necessária quanto à instalação, configuração e gerenciamento das soluções adquiridas.

3.91.1.12. A qualidade do repasse de conhecimento será avaliada pelos participantes ao final de sua realização e, caso sua qualidade seja considerada insuficiente, a CONTRATADA deverá reformular sua metodologia e providenciar realização de nova turma, até o alcance dos objetivos do repasse, sem ônus adicional para a CONTRATANTE.

## 3.92. ACORDO DE NÍVEL DE SERVIÇO PARA SOLUÇÕES DE SEGURANÇA

### 3.92.1. CARACTERÍSTICAS GERAIS

3.92.1.1. Um acordo de nível de serviço define os índices a serem atingidos para o cumprimento do conjunto de compromissos acordados entre CONTRATANTE e CONTRATADA;

3.92.1.2. Tais índices serão medidos e aplicados aos serviços contratados pelo CONTRATANTE e prestados pela CONTRATADA;

3.92.1.3. Semestralmente os dados de Nível de Serviço deverão ser apresentados ao CONTRATANTE, incluindo informações sobre ações e necessidades para a correção de desvios, visando atingir, manter e melhorar os níveis desejados.

3.92.1.4. A abrangência e o nível de detalhamento dos demonstrativos serão definidos conforme as necessidades identificadas pela CONTRATADA, podendo sofrer alterações ao longo do tempo, as quais serão encaminhadas ao CONTRATANTE via os processos de Gerenciamento do Nível de Serviço e de Mudanças do mesmo;

3.92.1.5. Para a medição dos índices de nível de serviços, serão considerados os seguintes conceitos:

3.92.1.6. Requisição: solicitação do CONTRATANTE para intervenção no ambiente gerenciado e previsto no escopo desta proposta. Cada requisição será identificada unicamente por meio de um código e será classificada conforme seu nível de severidade no momento da sua comunicação a CONTRATADA;

3.92.1.7. Severidade: nível de prioridade/emergência atribuído ou solicitado para a realização de um atendimento a uma requisição do CONTRATANTE ou do ambiente, conforme critérios descritos a seguir. Solicitações de alteração do nível de severidade poderão ser submetidas à CONTRATADA e, quando julgadas pertinentes pela mesma, serão prontamente atendidas.

3.92.1.7.1. SEVERIDADE CRÍTICO: A Plataforma de Segurança para Defesa Cibernética está totalmente parada ou inoperante;

3.92.1.7.2. SEVERIDADE ALTO: A Plataforma de Segurança para Defesa Cibernética está ativa, mas com inoperância da maioria de suas funcionalidades, causando um impacto negativo no ambiente de produção;

3.92.1.7.3. SEVERIDADE MÉDIO: A Plataforma de Segurança para Defesa Cibernética está operativa, mas suas funcionalidades são executadas com restrições;

3.92.1.7.4. SEVERIDADE BAIXO: A Plataforma de Segurança para Defesa Cibernética está operativa e a falha não compromete suas funcionalidades ou questões não tratadas pela documentação;

3.92.1.7.5. SEVERIDADE AGENDADO: O atendimento está relacionado apenas a esclarecimentos de dúvidas ou necessidade de informações da Plataforma de Segurança para Defesa Cibernética;

3.92.1.8. A cada chamado de suporte categorizado como Severidade Crítico ou Alto, o recurso humano designado para fornecer assistência na CONTRATADA deverá ser notificado e iniciará o auxílio na condução do processo internamente junto a CONTRATANTE;

3.92.1.9. Referente aos chamados categorizados como Severidade Crítico ou Alto, cabe a CONTRATADA dar início, junto ao CONTRATANTE, às providências que serão adotadas para a solução do chamado;

3.92.1.10. Para os chamados de suporte categorizado como Severidade Crítico ou Alto, o atendimento não pode ser interrompido até o completo restabelecimento de todas as funções do sistema paralisado (indisponível), mesmo que para isso tenham que se estender por períodos noturnos e dias não úteis (sábados, domingos e feriados), de acordo com a disponibilidade do CONTRATANTE.

| Severidade | Descrição |
|---|---|
| Agendado | Esclarecimento de dúvidas ou similar. |
| Baixo | A Plataforma de Segurança para Defesa Cibernética opera sem impacto de negócio. |

| | |
|---|---|
| Médio | A Plataforma de Segurança para Defesa Cibernética opera com degradação de desempenho. |
| Alto | A Plataforma de Segurança para Defesa Cibernética opera com paralisação parcial. |
| Crítico | A Plataforma de Segurança para Defesa Cibernética inoperante ou paralisação total. |

3.92.1.11. ***Tempo de Notificação:*** O tempo máximo para a NOTIFICAÇÃO da CONTRATANTE pela CONTRATADA, conforme a severidade do incidentes Críticos e Altos:

| Severidade | Descrição | Meta para tempo de resposta |
|---|---|---|
| Agendado | Esclarecimento de dúvidas ou similar. | 32 horas |
| Baixo | A Plataforma de Segurança para Defesa Cibernética opera sem impacto de negócio. | 16 horas |
| Médio | A Plataforma de Segurança para Defesa Cibernética opera com degradação de desempenho. | 8 horas |
| Alto | A Plataforma de Segurança para Defesa Cibernética opera com paralisação parcial. | 6 horas |
| Crítico | A Plataforma de Segurança para Defesa Cibernética inoperante ou paralisação total. | 4 horas |

3.92.1.12. Não se encaixam nos prazos descritos nos itens referentes aos níveis de criticidade, problemas cuja solução dependa de correção de falhas (bugs) ou da liberação de novas versões e patches de correção, desde que comprovados pelo fabricante da solução;

3.92.1.13. Os chamados escalados para o fabricante e em tratamento por aquele não se encaixam nos prazos descritos.

3.92.1.14. Serão excluídos do cálculo, os tempos de paralisação, decorrentes dos seguintes eventos:

3.92.1.15. Janela de manutenção acordada entre CONTRADADA e CONTRATANTE;

3.92.1.16. Falhas na infraestrutura provisionada pelo CONTRATANTE decorrentes de eventos como:

3.92.1.17. Perda de conexão com a rede corporativa;

3.92.1.18. Acidentes operacionais internos;

3.92.1.19. Falta de energia elétrica;

3.92.1.20. Incêndios, vazamentos e outros intempéries que envolvam o ambiente físico da CONTRATANTE;

3.92.1.21. Entende-se que haverá uma fase inicial de transição e adequação dos processos de atendimento por parte da CONTRATADA. Sendo assim, os níveis de serviço (SLAs) não serão exigidos contratualmente durante os primeiros 60 (sessenta) dias úteis de duração do contrato. Os índices deverão ser apurados e apresentados ao CONTRATANTE, no entanto, a CONTRATADA não estará sujeita a penalidades pelo seu descumprimento durante este período.

## 3.93. DA GARANTIA E SUPORTE TÉCNICO ESPECIALIZADO

### 3.93.1. CARACTERÍSTICAS DA GARANTIA DOS ITENS DA SOLUÇÃO

3.93.1.1. Todos os produtos ofertados devem ser novos, sem uso anterior e, estar em linha de produção e comercialização pelo fabricante dos mesmos no momento da proposta, não devendo haver anúncio de "fim de produção" (EOL - End-of-Life) nem de apresentação do fim de comercialização (EOS - End-of-Sales) até esta data;

3.93.1.2. Todos os itens ofertados devem possuir garantia e suporte durante o período do contrato de 12 (doze) meses com direito a atualização de firmware, troca de peças e abertura de chamados no fabricante. Tal procedimento se justifica pelo fato de que, de forma geral a contratação, a posteriori, de serviços de manutenção para ativos fora de garantia, usualmente é mais onerosa para a Administração do que quando o bem é adquirido com garantia para toda sua vida útil;

3.93.1.3. A garantia e suporte durante o período de contrato 12 (doze) meses deverá ser na modalidade 24x7x365, e troca de peças no próximo dia útil em horário comercial. O canal de chamados de suporte deverá ser responsável pelo hardware e software de modo global

empregados nesta solução integrada. O tempo de resposta máximo para um chamado técnico aberto com prioridade máxima deverá ser de 4 (quatro) horas e sem limites de requisições para suporte.

## 3.94. CARACTERÍSTICAS DO SUPORTE TÉCNICO DOS ITENS DA SOLUÇÃO

3.94.1. Entende-se por serviços de suporte técnico especializado, as ações corretivas que visam retomar a normalidade do ambiente em caso de indisponibilidade parcial e/ou total;

3.94.2. A CONTRATADA deverá possuir serviço de suporte técnico especializado com as seguintes características:

3.94.2.1. Central de atendimento através de canal 0800 operando em regime 24x7xAno, durante o período de contrato de garantia e suporte;

3.94.2.2. A CONTRATADA deverá disponibilizar Ferramenta de Acompanhamento de Chamados, de sua propriedade e de sua responsabilidade, que atendam aos seguintes requisitos:

3.94.2.2.1. O acesso às informações deverá ser protegido por senha e conexão segura ou outro método equivalente;

3.94.2.2.2. O CONTRATANTE deverá ter acesso à ferramenta via interface WEB;

3.94.2.2.3. A ferramenta deverá manter identificação do projeto ou demanda, data e hora de abertura do chamado, início e término do atendimento, identificação e resolução do escopo, documentação da solução, status, recursos alocados e outras informações pertinentes;

3.94.2.2.4. A ferramenta deverá ser capaz de exportar seus dados em formato csv;

3.94.2.2.5. A ferramenta deverá ser capaz de permitir a emissão de relatórios diários e/ou mensais para o controle de todas as solicitações abertas e encaminhadas pelo CONTRATANTE;

3.94.2.2.6. A ferramenta deverá ser capaz de gerir e garantir que os níveis de serviços de atendimento sejam monitorados, de forma que o tempo de atendimento de uma solicitação comece a ser contado a partir do envio da mesma pelo usuário solicitante e seja finalizado no momento de fechamento da solicitação no sistema;

3.94.2.3. Sistema de registro de chamados;

3.94.2.4. Capacidade para realização de diagnósticos (localmente ou remotamente);

3.94.2.5. Capacidade para acesso remoto do ambiente para resolução de problemas;

3.94.2.6. Deve possuir portal para consulta de status de chamados técnicos;

3.94.2.7. O portal deve permitir a extração de relatório em arquivos com extensão compatível com os softwares Word, Excel ou PDF;

3.94.2.8. Abertura e acompanhamento de chamados técnico junto ao fabricante da solução;

3.94.2.9. Intermediação entre CONTRATANTE e fabricante da solução para tratativas técnicas;

3.94.2.10. Intermediação no processo de troca de peças (RMA), caso necessário, agendamento de técnico local, acompanhamento durante a operação de troca e trâmite de devolução da peça com defeito;

3.94.2.11. Atualização de microcódigos e softwares que compõem a solução;

3.94.2.12. Configuração de novas funcionalidades da solução contratada;

3.94.2.13. Capacitação na modalidade “hands-on” durante a implementação da solução;

3.94.2.14. Análise periódica do ambiente (Health-Check);

3.94.2.15. Gerar relatório com sugestões de melhorias e suas aplicabilidades (capacity plan);

3.94.2.16. Implementação das melhorias recomendadas em conjunto com a equipe técnica da contratada;

3.94.2.17. Recapacitação técnica da equipe da CONTRATANTE quando houver novas funcionalidades na solução na modalidade “hands-on”;

3.94.2.18. Apoiar na aplicação das boas práticas para adequação de aplicações;

3.94.2.19. Análise e tratamento de alertas e eventos;

3.94.2.20. Análise de desempenho;

3.94.2.21. Disponibilizar canais para abertura de chamados técnicos via 0800 e WEB;

3.94.2.22. Apoiar na integração de softwares de terceiros com a solução;

3.94.2.23. Gerar matriz de compatibilidade para apoiar na migração e implementação de aplicações e serviços;

3.94.2.24. Apoiar no processo de migração de ambiente legado;

3.94.2.25. Demonstrar novas funcionalidades da solução;

3.94.2.26. Serviços de Suporte Técnico Especializado Remoto;

3.94.2.27. Em caso de necessidade, deve ser escalonado para o fabricante;

3.94.2.28. Recomendar solução de contorno, quando possível;

3.94.2.29. Obter e coordenar reparação de firmware e hardware que podem incluir instalação de patches e/ou service packs;

3.94.2.30. Documentar atividades de resolução;

3.94.2.31. Realizar configurações temporárias quando necessário para recuperar recursos que falharam e recomendar mudanças permanentes quando necessárias;

3.94.2.32. Acionar fornecedor ou terceiro para recuperação de recurso;

3.94.2.33. Prover um plano de ação para eventos;

3.94.2.34. Gerenciar a comunicação durante problemas;

3.94.2.35. Identificar, obter e coordenar instalação de firmware, patches, service packs etc. em conjunto com equipe da CONTRATANTE;

3.94.2.36. Analisar problemas em sistemas com o objetivo de identificar oportunidades de prever falhas futuras;

3.94.2.37. Rever recomendações com a CONTRATANTE durante a análise mensal ou conforme requisitado;

3.94.2.38. Alimentar / Documentar logs quando a manutenção for realizada ou correção/atualização de firmware, software, ou aplicação e patches de segurança quando implementados;

3.94.2.39. Documentar qualquer recomendação ou ação realizada;

3.94.2.40. Testar e verificar patches para testes de hardware antes da instalação na produção de dispositivo de armazenamento. Esses testes pré-produção serão realizados em conjunto com a CONTRATANTE;

3.94.2.41. Completar serviço padrão de configuração;

3.94.2.42. Comunicar e recomendar mudanças de configuração para a CONTRATANTE;

3.94.2.43. Coordenar a instalação, configuração e upgrades em conjunto com equipe da CONTRATANTE;

3.94.2.44. Manter documentação de sistema e hardware para o ambiente e prover revisão mensal ou conforme requisitado pela CONTRATANTE, respeitando, inclusive, formatação dadocumentação, caso estipulado.

3.95. ONDIÇÕES DE FORNECIMENTO

3.95.1. O CONTRATANTE deverá ser comunicado antecipadamente sobre a data e o horário da entrega de toda a solução. Não serão aceitos produtos e serviços que estiverem em desacordo com as especificações constantes neste instrumento.

3.95.2. O fornecedor será responsável por todos os ônus relativos ao fornecimento da solução, incluindo frete, seguro, carga e descarga, desde a origem até o local estipulado neste Termo.

3.95.3. Todos os itens que compõem o objeto desta aquisição deverão ser fornecidos, obrigatoriamente, por um único licitante, em virtude da complexidade do projeto.

3.95.4. O prazo para a entrega da solução será de 90 (noventa) dias úteis, contados a partir da assinatura do contrato pela CONTRATADA.

## 4. DOS PRAZOS DE VIGÊNCIA E EXECUÇAO

4.1. O início dos serviços ocorrerá mediante a expedição da Ordem de Serviço, que será emitida pelo Município contratante, com prazo máximo de 10 (dez) dias úteis para o início do cumprimento.

4.2. Os demais prazos de duração e entrega estão especificados no item 3 deste Termo de Referência.

## 5. DO VALOR, DESCONTOS MÍNIMOS ACEITÁVEIS E CRITÉRIO DE JULGAMENTO

5.1. O PREÇO MÁXIMO ACEITO para a aquisição, conforme os orçamentos coletados, é o valor estimado de R$ 96.189.254,53 (noventa e seis milhões, cento e oitenta e nove mil, duzentos e cinquenta e quatro reais e cinquenta e três centavos).

| LOTE | ITEM | DESCRIÇÃO | UNIDADE | QTD | VALOR MENSAL | VALOR TOTAL |
|---|---|---|---|---|---|---|
| | 1 | Serviço de armazenamento | SERVIÇO | 48 | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 01 | | inteligente | | | R$ 1.756.246,67 | R$ 21.074.960,02 |
| | 2 | Expansão de serviço de armazenamento inteligente | SERVIÇO | 100 | R$ 1.192.186,99 | R$ 14.306.243,84 |
| | 3 | Serviço de proteção de dados | SERVIÇO | 38 | R$ 516.298,91 | R$ 6.195.586,93 |
| | 4 | Serviço de movimentação de dados | SERVIÇO | 38 | R$ 64.906,08 | R$ 778.872,97 |
| | 5 | Serviço de transbordo de cópias de segurança – Tipo Quente | SERVIÇO | 48 | R$ 901.193,91 | R$ 10.814.326,91 |
| | 6 | Serviço de conectividade | SERVIÇO | 96 | R$ 1.187.747,39 | R$ 14.252.968,68 |
| | 7 | Serviço de monitoramento e gerenciamento de soluções de segurança da informação, com inteligência de ameaças para 1 domínio, através de Centro de Operação de Segurança 24x7 da contratada. | SERVIÇO | 38 | R$ 119.706,29 | R$ 1.436.475,54 |
| | 8 | Serviço de proteção de perímetro – Pacote de 1 ativo. | SERVIÇO | 96 | R$ 617.683,77 | R$ 7.412.205,21 |
| | 9 | Serviço de proteção de endpoints/servidores com correlacionamento de eventos – Pacote de 150 ativos. | SERVIÇO | 38 | R$ 164.187,98 | R$ 1.970.255,71 |
| | 10 | Serviço de gestão de vulnerabilidades – Pacote de 150 ativos. | SERVIÇO | 38 | R$ 558.162,82 | R$ 6.697.953,85 |
| | 11 | Serviço de gerenciamento de acesso a contas privilegiadas com cofre de senhas – Pacote de 150 ativos. | SERVIÇO | 38 | R$ 542.476,15 | R$ 6.509.713,77 |
| | 12 | Serviço de Teste de Penetração – 3000 horas de Serviço. | SERVIÇO | 38 | R$ 121.082,39 | R$ 1.452.988,64 |
| | 13 | Serviços Gerenciados de Infraestrutura. | SERVIÇO | 38 | R$ 118.340,35 | R$ 1.420.084,15 |
| | 14 | Serviço de transbordo de cópias de segurança – Tipo Frio. | SERVIÇO | 48 | R$ 33.006,70 | R$ 396.080,37 |
| | 15 | Serviços de conversão de aplicações | SERVIÇO | 38 | R$ 122.544,83 | R$ 1.470.537,94 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | em tecnologias de container. | | | | |

## 6. DAS OBRIGAÇÕES DA CONTRATADA

6.1. São obrigações da licitante CONTRATADA:

6.2. Manter as condições de habilitação e qualificação exigidas na licitação durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, incluindo a comprovação de regularidade fiscal e trabalhista junto ao Órgão Gerenciador.

6.3. Indicar preposto aceito pelo Órgão Participante para representá-lo na execução do contrato e informar à CONTRATANTE quem será o responsável pelos contatos e tratativas.

6.4. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, qualquer objeto do contrato que apresente vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados.

6.5. Responsabilizar-se integralmente pela locação contratada e pelo controle de qualidade dos serviços executados, bem como solucionar qualquer irregularidade relacionada aos equipamentos locados e/ou aos serviços prestados.

6.6. Ressarcir danos causados diretamente à administração ou a terceiros, decorrentes de culpa ou dolo na execução do contrato, sem que a fiscalização ou o acompanhamento pelo CONTRATANTE exima ou reduza essa responsabilidade.

6.7. Pagar todas as obrigações fiscais, previdenciárias, comerciais e trabalhistas decorrentes das atividades envolvidas no escopo dos serviços contratados, assegurando que os equipamentos estão livres de quaisquer ônus ou pendências judiciais ou extrajudiciais.

6.8. Substituir o bem ou serviço que estiver danificado ou em desconformidade com as especificações, tanto no momento da entrega quanto após a identificação de defeitos pela CONTRATANTE.

6.9. Responsabilizar-se pela correta disposição e descarte de resíduos, conforme a legislação ambiental vigente, sem causar danos ao meio ambiente, e cumprir integralmente todas as normativas legais relativas à proteção ambiental.

6.10. Atender prontamente a qualquer exigência de fiscalização inerente ao objeto do contrato, relatando à CONTRATANTE toda e qualquer irregularidade observada durante a execução do contrato.

6.11. Emitir Nota Fiscal dos produtos e/ou serviços realizados, discriminando-os individual e pormenorizadamente, especificando quantitativos, marcas e modelos, e destacando todos os tributos passíveis de retenção pelos órgãos participantes, conforme a legislação vigente.

6.12. Manter as condições de habilitação e qualificação exigidas na licitação, bem como comprovar a regularidade fiscal e trabalhista junto ao Órgão Gerenciador.

6.13. Enviar por e-mail o arquivo XML oriundo da emissão do DANFE para os endereços eletrônicos de cada Órgão Participante.

6.14. Acusar o recebimento de Autorizações de Fornecimento e notificações enviadas por meio eletrônico no prazo máximo de 24 horas, prorrogado para o próximo dia útil em caso de fim de semana ou feriado.

6.15. Emitir Nota Fiscal referente aos produtos e/ou serviços prestados, discriminando-os de forma individual e detalhada, especificando quantitativos, marcas e modelos.

6.16. A Nota Fiscal emitida deverá conter o destaque do valor de todos os tributos passíveis de retenção pelos Órgãos Participantes, nos termos da legislação vigente, especialmente o Imposto de Renda Retido na Fonte (IRRF), conforme a Instrução Normativa RFB nº 1.234/2012.

## 7. DAS OBRIGAÇÕES DOS ORGÃOS PARTICIPANTES/CONTRATANTES

7.1. São obrigações dos ORGÃOS PARTICIPANTES/CONTRATANTES:

7.2. Realizar o pagamento dos produtos e serviços contratados nos prazos, forma e condições estipuladas, conforme previsto no contrato.

7.3. Fiscalizar os fornecimentos e a execução dos serviços contratados, designando servidor para acompanhar e receber as obras e serviços, bem como relatar problemas e circunstâncias para facilitar a execução e garantir a boa qualidade dos serviços.

7.4. Indicar prepostos para contato com os responsáveis da empresa CONTRATADA, zelando pela comunicação eficiente entre as partes.

7.5. Prestar todos os esclarecimentos necessários para a prestação adequada dos serviços contratados, garantindo à CONTRATADA a fidelidade das informações e o acesso à documentação técnica para que os serviços se desenvolvam sem percalços.

7.6. Zelar pela boa execução do contrato, cumprindo todas as obrigações previstas no edital, seus anexos, e na forma da lei, além de garantir o cumprimento das obrigações previstas para a CONTRATADA.

7.7. Proporcionar todas as condições necessárias para a execução do contrato, comunicando, por escrito e tempestivamente, quaisquer mudanças necessárias para a boa execução dos serviços.

7.8. Garantir a gestão junto aos órgãos públicos afins, concessionárias e empresas privadas para liberar as áreas onde os serviços serão realizados, abrangendo ações como isolar, proteger áreas e circuitos, emitir licenças e promover condições para que os serviços possam ser executados sem interrupção.

7.9. Velar pela manutenção do equilíbrio econômico-financeiro do contrato durante sua execução, inclusive em casos de eventual paralisação dos serviços.

7.10. Cumprir integralmente as obrigações previstas no edital e nesta ata, bem como zelar pelo cumprimento das obrigações impostas à contratada.

7.11. Observar e cumprir as demais disposições constantes neste edital, em seus anexos, e conforme o disposto na legislação aplicável.

## 8. PRAZO DE VIGÊNCIA DA ATA DE REGISTRO DE PREÇOS

8.1. A Ata de Registro de Preços terá validade de 1 (um) ano, podendo ser prorrogada por igual período, desde que comprovada a vantagem econômica, nos termos do que dispõe o art. 84 da Lei nº 14.133/2021, que estabelece a possibilidade de prorrogação desde que demonstrado o interesse público e a vantagem econômica, assegurando a manutenção das condições vantajosas para a Administração Pública.

## 9. DA DOTAÇÃO ORÇAMENTÁRIA

9.1. As despesas decorrentes da execução do objeto contratual correrão à conta da dotação orçamentária designada pelo município consorciado que celebrar o contrato com a licitante vencedora, conforme as previsões orçamentárias específicas de cada ente CONTRATANTE.

## 10. DA MODALIDADE

10.1. Em licitações de registro de preços, a modalidade licitatória deverá ser pregão ou concorrência, conforme previsto no inciso XLV do art. 6º da Lei nº 14.133, de 1º de abril de 2021:

> *Art. 6º Para os fins desta Lei, consideram-se:*
>
> *XLV sistema de registro de preços: conjunto de procedimentos para realização, mediante contratação direta ou licitação nas modalidades pregão ou concorrência, de registro formal de preços relativos a prestação de serviços, a obras e a aquisição e locação de bens para contratações futuras;*

10.2. E, também, no art. 14º do Decreto Federal 11.462/2023:

> *Art. 14. O processo licitatório para registro de preços será realizado na modalidade concorrência ou pregão.*

> *O pregão consiste em modalidade de licitação obrigatória destinada à aquisição de bens ou serviços comuns e atualmente é disciplinado pela Lei 14.133 de 1º de abril de 2021, aplicável a todos os entes federativos (União, Estados, Distrito Federal e Municípios, tanto à administração direta quanto indireta).*

10.3. Bens e serviços comuns, conforme definição constante do inciso XIII do art. 6º da Lei 14.133/21, são "aqueles cujos padrões de desempenho e qualidade possam ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado".

10.4. E os requisitos para a adoção do Sistema de Registro de Preços encontram-se no artigo 82º do Decreto Federal n. 11.462/2023:

> *"Art. 82.[...]*
>
> *§ 5º O sistema de registro de preços poderá ser usado para a contratação de bens e serviços, inclusive de obras e serviços de engenharia, observadas as seguintes condições:*
>
> *I realização prévia de ampla pesquisa de mercado;*
>
> *II seleção de acordo com os procedimentos previstos em regulamento;*
>
> *III desenvolvimento obrigatório de rotina de controle;*
>
> *IV atualização periódica dos preços registrados;*
>
> *V definição do período de validade do registro de preços;*
>
> *VI inclusão, em ata de registro de preços, do licitante que aceitar cotar os bens ou serviços em preços iguais aos do licitante vencedor na sequência de classificação da licitação e inclusão do licitante que mantiver sua proposta original.*
>
> *§ 6º O sistema de registro de preços poderá, na forma de regulamento, ser utilizado nas hipóteses de inexigibilidade e de dispensa de licitação para a aquisição de bens ou para a contratação de serviços por mais de um órgão ou entidade."*

10.5. Assim sendo, considerando que os requisitos para utilização do sistema de registro de preços encontram-se preenchidos, justifica-se a adoção da modalidade pregão na forma eletrônica para o registro de preços dos serviços acima identificados.

## 11. CLASSIFICAÇÃO DOS SERVIÇOS/BENS COMUNS

11.1. Os bens/serviços ora pretendidos e considerados comuns de acordo com o Art. 6, inciso "XIII", da Lei Federal nº 14.133/21.

> *"Art. 6, Inciso XIII bens e serviços comuns: aqueles cujos padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado".*

## 12. DA SUBCONTRATAÇÃO

12.1. Não será admitida a subcontratação do objeto licitatório, desde que observados os limites estabelecidos em lei.

Alfenas/MG, 13 de setembro de 2024.

Responsáveis pela elaboração do Termo de Referência:

Nelson Daniel da Costa Júnior
Consultor em Tecnologia

Carlos Leandro Zétula
Consultor em Tecnologia

De acordo:

Fausto Costa

Departamento de Contas

CIMLAGO

ANEXO II – MODELO DE PROPOSTA DE PREÇOS

EDITAL DO PREGÃO, NA FORMA ELETRÔNICA, Nº 016/2024

PROCESSO ADMINISTRATIVO LICITATÓRIO ELETRÔNICO 016/2024

SISTEMA DE REGISTRO DE PREÇOS

Apresentamos nossa proposta para aquisição do objeto da presente licitação Pregão, na Forma Eletrônica acatando todas as estipulações consignadas no respectivo Edital e seus anexos.

## 1. IDENTIFICAÇÃO DO PROPONENTE:

NOME DA EMPRESA:

CNPJ e INSCRIÇÃO ESTADUAL:

REPRESENTANTE e CARGO:

CARTEIRA DE IDENTIDADE e CPF:

ENDEREÇO, TELEFONE E E-MAIL:

## 1. PROPOSTA DE PREÇOS

| LOTE | ITEM | DESCRIÇÃO | UNIDADE | QTD | VALOR MENSAL | VALOR TOTAL |
|---|---|---|---|---|---|---|
| 01 | 1 | Serviço de armazenamento inteligente | SERVIÇO | 48 | | |
| | 2 | Expansão de serviço de armazenamento inteligente | SERVIÇO | 100 | | |
| | 3 | Serviço de proteção de dados | SERVIÇO | 38 | | |
| | 4 | Serviço de movimentação de dados | SERVIÇO | 38 | | |
| | 5 | Serviço de transbordo de cópias de segurança – Tipo Quente | SERVIÇO | 48 | | |
| | 6 | Serviço de conectividade | SERVIÇO | 96 | | |
| | 7 | Serviço de monitoramento e gerenciamento de soluções de segurança da informação, com inteligência de ameaças para 1 domínio, através de Centro de Operação de | SERVIÇO | 38 | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | Segurança 24x7 da contratada. | | | | |
| | 8 | Serviço de proteção de perímetro – Pacote de 1 ativo. | SERVIÇO | 96 | | |
| | 9 | Serviço de proteção de endpoints/servidores com correlacionamento de eventos – Pacote de 150 ativos. | SERVIÇO | 38 | | |
| | 10 | Serviço de gestão de vulnerabilidades – Pacote de 150 ativos. | SERVIÇO | 38 | | |
| | 11 | Serviço de gerenciamento de acesso a contas privilegiadas com cofre de senhas – Pacote de 150 ativos. | SERVIÇO | 38 | | |
| | 12 | Serviço de Teste de Penetração – 3000 horas de Serviço. | SERVIÇO | 38 | | |
| | 13 | Serviços Gerenciados de Infraestrutura. | SERVIÇO | 38 | | |
| | 14 | Serviço de transbordo de cópias de segurança – Tipo Frio. | SERVIÇO | 48 | | |
| | 15 | Serviços de conversão de aplicações em tecnologias de container. | SERVIÇO | 38 | | |

## 2. CONDIÇÕES GERAIS

2.1 A proponente declara conhecer os termos do instrumento convocatório que rege a presente licitação.

## 3. VALIDADE DA PROPOSTA COMERCIAL

De no mínimo, **90 (noventa) dias** contados a partir da data da sessão pública do Pregão.

## 4. PRAZO DE VALIDADE DA ATA DE REGISTRO DE PREÇOS

De **12 (doze) meses**, podendo ser prorrogado.

**Obs.:** Nos preços cotados estão incluídos todos os custos diretos e indiretos necessários à perfeita execução do objeto, composição do BDI, entregas nos municípios consorciados, encargos sociais e inclusive as despesas com materiais e/ou equipamentos fornecidos, mão de obra especializada ou não, fretes, seguros em geral, equipamentos auxiliares, ferramentas,

encargos da Legislação Tributária, Social, Trabalhista e Previdenciária, da infortunística do trabalho e responsabilidade civil por quaisquer danos causados a terceiros ou dispêndios resultantes de impostos, taxas, regulamentos e posturas municipais, estaduais e federais, enfim, tudo o que for necessário para a execução total e completa do objeto desta licitação.

Local e Data

Nome e Assinatura do Representante da Empresa

ANEXO III – DADOS DO LICITANTE

EDITAL DO PREGÃO, NA FORMA ELETRÔNICA, Nº 016/2024

PROCESSO ADMINISTRATIVO LICITATÓRIO ELETRÔNICO 016/2024

SISTEMA DE REGISTRO DE PREÇOS

1. DADOS BANCÁRIOS:

| |
|---|
| NOME DO BANCO: |
| |
| CIDADE: |
| |
| Nº DA AGÊNCIA: |
| |
| Nº DA CONTA CORRENTE DA EMPRESA: |
| |
| NOME DA CONTA CORRENTE: |
| |
| CHAVE PIX: |

2. DADOS DO REPRESENTANTE LEGAL RESPONSÁVEL PELA ASSINATURA DAS ATAS

| |
|---|
| NOME COMPLETO: |
| |
| CARGO OU FUNÇÃO: |
| |
| IDENTIDADE Nº: |
| |
| CPF/MF Nº: |
| |

| |
|---|
| TELEFONE PARA CONTATO: |

## 3. DECLARAÇÃO DE DOMICÍLIO ELETRÔNICO DA EMPRESA

| |
|---|
| Declaramos que o Domicílio Eletrônico da Empresa para o recebimento de autorizações de fornecimento, alerta de avisos, notificações e decisões administrativas, é: |
| E-MAIL: |

Obs.: *Informar apenas 1 (um) e-mail como domicílio eletrônico da empresa. Havendo mais de um e-mail informado, será considerado somente o primeiro da lista.*

## 4. DECLARAÇÃO DE ASSINATURA POR CERTIFICAÇÃO DIGITAL

| |
|---|
| Declaramos estar ciente que, o representante legal indicado neste documento, será o signatário da "Ata de Registro de Preço", o qual deverá assinar o documento eletrônico em formato "PDF", por certificação digital, caso assim solicitado, bem como somente serão autorizados os pagamentos em contas cujo CNPJ de titularidade seja idêntico àquele da habilitação e proposta vinculada, na licitação, salvo em caso de participação<br>em consórcio de empresas, quando permitido no instrumento convocatório. |

Local e Data

Nome e Assinatura do Representante da Empresa

## ANEXO IV – DECLARAÇÃO DE CUMPRIMENTO PLENO DOS REQUISITOS DE HABILITAÇÃO

## EDITAL DO PREGÃO, NA FORMA ELETRÔNICA, Nº 016/2024

PROCESSO ADMINISTRATIVO LICITATÓRIO ELETRÔNICO 016/2024

SISTEMA DE REGISTRO DE PREÇOS

_____(RAZÃO SOCIAL DA EMPRESA) _____ CNPJ nº _____, sediada em _____(ENDEREÇO COMERCIAL)_____, declara, sob as penas da Lei Federal nº 14.133, de 2021, que cumpre plenamente os requisitos para sua habilitação no presente processo licitatório.

**OBS –** Se for Microempresa ou Empresa de Pequeno Porte – EPP com problemas na habilitação, fazer constar tal ressalva.

Local e Data

Nome e Assinatura do Representante da Empresa

## ANEXO V – DECLARAÇÃO DE AUSÊNCIA DE CONDENAÇÃO

## EDITAL DO PREGÃO, NA FORMA ELETRÔNICA, Nº 016/2024

PROCESSO ADMINISTRATIVO LICITATÓRIO ELETRÔNICO 016/2024

SISTEMA DE REGISTRO DE PREÇOS

_____(RAZÃO SOCIAL DA EMPRESA) _____ CNPJ nº _____, sediada em _____(ENDEREÇO COMERCIAL)_____, declara, sob as penas da Lei Federal nº 14.133, 2021, que nos 5 (cinco) anos anteriores à divulgação do edital, não foi 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.

Local e Data

Nome e Assinatura do Representante da Empresa

## ANEXO VI – DECLARAÇÃO DE AUSÊNCIA DE VÍNCULO

## EDITAL DO PREGÃO, NA FORMA ELETRÔNICA, Nº 016/2024

PROCESSO ADMINISTRATIVO LICITATÓRIO ELETRÔNICO 016/2024

SISTEMA DE REGISTRO DE PREÇOS

_____(RAZÃO SOCIAL DA EMPRESA) _____ CNPJ nº _____, sediada em _____(ENDEREÇO COMERCIAL)_____, declara, sob as penas da Lei Federal nº 14.133, 2021, que não mantem 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.

Local e Data

Nome e Assinatura do Representante da Empresa

ANEXO VII – DECLARAÇÃO DE MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE

EDITAL DO PREGÃO, NA FORMA ELETRÔNICA, Nº 016/2024

PROCESSO ADMINISTRATIVO LICITATÓRIO ELETRÔNICO 016/2024

SISTEMA DE REGISTRO DE PREÇOS

A empresa _____, inscrita no CNPJ sob o nº _____, por intermédio de seu representante legal, o(a) Sr.(a.) ou procurador _____, portador(a) da Carteira de Identidade nº ___, do CPF nº _____, DECLARA, sob as penas elencadas na Lei Federal n° 14.133, de 2021, que em conformidade com o previsto no art. 3° da Lei Complementar n° 123, de 15 de dezembro de 2006, ter a receita bruta equivalente a uma _____(microempresa ou empresa de pequeno porte). Declara ainda que não há nenhum dos impedimentos previstos no § 4°, art. 3° da LC 123/06.

Local e Data

Nome e Assinatura do Representante da Empresa

ANEXO VIII – DECLARAÇÃO DE ENQUADRAMENTO DE RECEITA BRUTA PARA FINS DE BENEFÍCIO PREVISTO NA LEI COMPLEMENTAR FEDERAL 123/2006

EDITAL DO PREGÃO, NA FORMA ELETRÔNICA, Nº 016/2024

PROCESSO ADMINISTRATIVO LICITATÓRIO ELETRÔNICO 016/2024

SISTEMA DE REGISTRO DE PREÇOS

A empresa _____, inscrita no CNPJ sob o nº _____, por intermédio de seu representante legal, o(a) Sr.(a.) ou procurador _____, portador(a) da Carteira de Identidade nº _____ _____, do CPF nº _____, DECLARA, sob as penas elencadas na Lei Federal n° 14.133, de 2021, que não celebrou Contratos com a Administração Pública cujos valores somados extrapolou a receita bruta máxima admitida para fins de enquadramento como Empresa de Pequeno Porte no ano-calendário desta licitação, em conformidade com o previsto no inciso II, do art. 3° da Lei Complementar n° 123, de 15 de dezembro de 2006 e § 2º, do art. 4º, da Lei Federal nº 14.133, de 2021.

Local e Data

Nome e Assinatura do Representante da Empresa

ANEXO IX – DECLARAÇÃO DE CUMPRIMENTO DO ARTIGO 7º, INCISO XXXIII, DA CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL

EDITAL DO PREGÃO, NA FORMA ELETRÔNICA, Nº 016/2024

PROCESSO ADMINISTRATIVO LICITATÓRIO ELETRÔNICO 016/2024

SISTEMA DE REGISTRO DE PREÇOS

_____, inscrito no CNPJ n°_____, por intermédio de seu representante legal o(a) Sr(a)._____, portador(a) da de Identidade nº____e do CPF nº _____, DECLARA, para fins do disposto no inciso V do artigo 68, da Lei Federal nº 14.133, de 2021, que não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre, e não emprega menor de dezesseis anos (art. 7º, inciso XXXIII, da Constituição Federal).

Ressalva: emprega menor, a partir de quatorze anos, na condição de aprendiz (  ). (Observação: em caso afirmativo, assinalar a ressalva acima)

Local e Data

Nome e Assinatura do Representante da Empresa

## ANEXO X – DECLARAÇÃO DE RESERVA DE CARGOS

## EDITAL DO PREGÃO, NA FORMA ELETRÔNICA, Nº 016/2024

PROCESSO ADMINISTRATIVO LICITATÓRIO ELETRÔNICO 016/2024

SISTEMA DE REGISTRO DE PREÇOS

(RAZÃO SOCIAL DA EMPRESA) _____ CNPJ nº _____, sediada em (ENDEREÇO COMERCIAL)_____, declara, sob as penas da Lei Federal nº 14.133, de 2021, 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.

Observação: Os licitantes que, por sua natureza ou por força de lei, estiverem dispensados do cumprimento da reserva de cargos descrito nesta declaração, deverão apresentar declaração identificando a situação e citando os dispositivos legais pertinentes.

Local e Data

Nome e Assinatura do Representante da Empresa

ANEXO XI – MINUTA DA ATA DE REGISTRO DE PREÇOS N° ___/2024

EDITAL DO PREGÃO, NA FORMA ELETRÔNICA, Nº 016/2024

PROCESSO ADMINISTRATIVO LICITATÓRIO ELETRÔNICO 016/2024

SISTEMA DE REGISTRO DE PREÇOS

Aos ___ dias do mês de _____ do ano de dois mil e vinte e quatro, presentes de um lado, o Consórcio Intermunicipal Multifinalitário dos Municípios do Lago de Furnas CIMLAGO, consórcio público multifinalitário, com personalidade jurídica de direito público, inscrito no CNPJ sob o nº 50.387.580/0001-90, com sede na Rua Juscelino Barbosa, nº 816, Centro, em Alfenas, Estado de Minas Gerais – CEP 37.130-039, neste ato representado por sua Presidente, Sra. Luiza Maria Lima Menezes, Prefeita do Município de Nepomuceno/MG, doravante denominado ORGÃO GERENCIADOR, e os Municípios de: Aguanil/MG, Alfenas/MG, Alpinópolis/MG, Alterosa/MG, Areado/MG, Boa Esperança/MG, Cabo Verde/MG, Camacho/MG, Campo do Meio/MG, Campos Gerais/MG, Cana Verde/MG, Candeias/MG, Capitólio/MG, Carmo do Rio Claro/MG, Conceição da Aparecida/MG, Coqueiral/MG, Cristais/MG, Divisa Nova/MG, Elói Mendes/MG, Fama/MG, Formiga/MG, Guapé/MG, Ilicínea/MG, Juruaia/MG, Lavras/MG, Machado/MG, Muzambinho/MG, Nepomuceno/MG, Paraguaçu/MG, Perdões/MG, Pimenta/MG, Poço Fundo/MG, Ribeirão Vermelho/MG, São João Batista do Glória/MG, São José da Barra/MG, Serrania/MG, Três Pontas/MG e Varginha/MG, doravante denominados ORGÃOS PARTICIPANTES do Sistema de Registro de Preços, e passam a integrar a Ata de Registro de Preços após manifestação, RESOLVEM registrar os preços da empresa _____, pessoa jurídica de direito privado, situada na _____, nº ____, na cidade de _____, inscrita no CNPJ sob o nº _____, neste ato representada pelo Sr. _____, doravante denominada FORNECEDOR, para fornecimento parcelado dos itens constantes do objeto a seguir, sujeitando-se as partes às determinações das Resoluções 004/2024 e 006/2024, da Lei Federal nº 14.133, de 2021, e nos casos omissos.

## 1. CLÁUSULA PRIMEIRA – DO OBJETO

1.1. A presente Ata tem como objeto o REGISTRO DE PREÇOS, por meio de licitação compartilhada, para a eventual e futura aquisição de infraestrutura como serviço, abrangendo soluções de armazenamento inteligente, proteção e armazenamento de dados, soluções de redes, proteção de perímetro, endpoint e gerenciamento de vulnerabilidades, com a finalidade de proporcionar ampla capacidade de atendimento aos usuários dos sistemas, incluindo serviços de instalação, configuração, transferência de conhecimento técnico e gerenciamento do ambiente, destinados a suprir futuras demandas, conforme especificações e condições estabelecidas no Anexo I e demais disposições do Edital, para atender os municípios consorciados ao Consórcio Intermunicipal Multifinalitário dos Municípios do Lago de Furnas – CIMLAGO, durante o prazo de validade da Ata de Registro de Preços, durante o prazo de validade da Ata de Registro de Preços, conforme itens da tabela da clausula décima sexta.

## 2. CLÁUSULA SEGUNDA – ESTIMATIVA DE CONSUMO/REMANEJAMENTO

2.1. Durante o prazo de validade da Ata de Registro de Preço, a estimativa de consumo será de acordo com a tabela da clausula décima sétima.

2.2. As alterações dos quantitativos dos itens serão realizadas através do remanejamento interno entre os Órgãos participantes.

2.2.1. Cabe ao Órgão gerenciador controlar, autorizar e operar a realização do remanejamento dos quantitativos dos itens internamente entre Órgãos Participantes.

2.3. Os Órgãos Participantes poderão adquirir de mais de um fornecedor, segundo a ordem de classificação, desde que razões de interesse público justifiquem e que o fornecedor registrado não possua capacidade de fornecimento compatível com o solicitado.

## 3. CLÁUSULA TERCEIRA – DAS ENTREGAS/EXECUÇÃO

3.1 O Contrato decorrente do Sistema de Registro de Preços SRP deverá ser realizado no

prazo de validade da Ata de Registro de Preços.

3.1.1 A contratação do item, com fornecimento parcelado, será efetuada conforme a necessidade do Órgão Participante.

3.1.2 A contratação com os fornecedores registrados será formalizada pelo Órgão Participante por intermédio de emissão de nota de empenho de despesa e autorização de fornecimento de compra.

3.1.3 **Os serviços e/ou itens contratados deverão ser prestados e/ou entregues de acordo com os prazos estabelecidos no Anexo I – Termo de Referência, considerando a complexidade inerente à prestação dos serviços objeto deste processo licitatório.**

3.1.4 O Fornecedor deverá entregar os itens constantes da autorização no local indicado pelo Órgão participante, com a respectiva Nota Fiscal Eletrônica e enviar o arquivo PDF/XML para o e-mail indicado nas Autorizações de Fornecimento.

3.1.5 Os recebimentos provisórios e definitivos ficarão sob a responsabilidade de cada Órgão Participante.

3.2 Todas as despesas relacionadas com as entregas em cada Órgão participante correrão por conta do Fornecedor.

3.2.1 Ficará sob total responsabilidade das proponentes vencedoras, realizar o transporte adequado e manter em perfeitas condições de armazenamento todos os materiais a serem entregues, garantindo a sua total eficiência e qualidade.

3.2.2 Todos os custos relacionados à execução da garantia ou troca de produtos correrão por conta exclusiva do fornecedor, incluídos os custos de transporte, troca de peças/equipamentos, horas técnicas, deslocamento de pessoal.

3.3 Na ausência de previsão na folha de dados, o prazo de garantia dos bens ofertados será de no mínimo **3 (três) meses** contados a partir da efetiva entrega dos bens à

administração. Mesmo que porventura alguma normativa diminuir o prazo de garantia estipulado neste Edital, permanecerá o prazo que for maior e que beneficiar o CONTRATANTE.

3.4 As exigências quanto a aplicação da garantia, deverão estar de acordo com o disposto no Termo de Referência.

## 4. CLÁUSULA QUARTA – DOS PAGAMENTOS

4.1 O pagamento pelas aquisições, objeto da presente licitação, será feito pelo Órgão Participante em favor da licitante vencedora, mediante transferência bancária (TED, DOC, depósito ou PIX) em conta corrente de titularidade do Fornecedor ou boleto, após as entregas dos bens, acompanhados da respectiva nota fiscal.

4.1.1 O Órgão Participante efetuará o pagamento em até 30 (trinta) dias, após a data de recebimento dos materiais, objeto desta Ata, acompanhado da respectiva Nota Fiscal Eletrônica e arquivo XML.

4.1.2 As taxas bancárias (TED, DOC, PIX ou outras) não poderão ser descontadas do pagamento previsto neste item.

4.1.3 Somente serão autorizados os pagamentos em contas cujo CNPJ de titularidade seja idêntico àquele da proposta vinculada, sendo responsabilidade da licitante manter a identidade de informação no momento do cadastro e durante a execução.

4.1.3.1 Se a Licitante Vencedora for empresa em forma de consórcios ou grupos de empresas que tenha participado nos termos do edital, os pagamentos serão realizados no CNPJ de sua constituição formal, o qual deverá ser apresentado como condição de assinatura da Ata de Registro de Preços.

4.1.3.2 Poderão ser realizados pagamentos em contas cujo CNPJ de titularidade seja diverso daquele da habilitação e proposta vinculada no caso de solicitação de alteração entre o CNPJ da matriz e filiais ou de filiais entre si, mediante comprovação do preenchimento dos

requisitos de habilitação pelo novo CNPJ.

4.1.4 Na realização do pagamento serão retidos os Tributos devidos conforme as normas em vigor e passíveis de retenção pelo Órgão Participante, devendo o fornecedor indicar estes valores no documento fiscal. Referente ao IRRF deverá ser observada a IN RFB 1.234/2012.

4.2 O número do CNPJ Cadastro Nacional de Pessoa Jurídica constante das notas fiscais deverá ser aquele fornecido na fase de habilitação do processo licitatório ao qual está vinculada esta ATA, salvo nos casos supracitados de consórcio de empresas e entre matrizes e filiais.

4.3 Nenhum pagamento será efetuado ao FORNECEDOR enquanto pendente de liquidação qualquer obrigação financeira ou técnica que lhe for imposta, em virtude de penalidade ou inadimplência, sem que isso gere direito ao pleito do reajustamento de preços ou correção monetária.

4.4 Os preços não serão reajustados durante a validade desta Ata de Registro de Preços, mesmo em caso de prorrogação, mas poderão ser revistos, na forma do edital e da cláusula oitava, desta ata.

4.5 Se o Órgão Participante não efetuar o pagamento no prazo previsto no Edital e na Ata de Registro de Preços, e tendo o Fornecedor, à época, adimplido integralmente as obrigações avençadas, inclusive quanto aos documentos que devem acompanhar a Nota Fiscal, os valores devidos serão monetariamente atualizados, a partir do dia de seu vencimento e até o dia de sua liquidação, segundo os mesmos critérios adotados para atualização de obrigações tributárias, conforme estabelecido no artigo 92, inciso V, da Lei Federal nº 14.133, de 2021.

## 5. CLÁUSULA QUINTA – DAS OBRIGAÇÕES DAS PARTES

5.1 Será de responsabilidade do Fornecedor cumprir todas as obrigações constantes nesta ata, no Edital, seus anexos e sua proposta, sob pena de aplicação das sanções previstas na cláusula sexta, assumindo exclusivamente seus os riscos e as despesas decorrentes da boa e

perfeita execução do objeto e, ainda:

a) fornecer o objeto deste Edital, de acordo com as especificações exigidas.

b) fornecer o objeto desta licitação, na forma, nos locais, nos prazos e nos preços estipulados na sua proposta;

c) prestar garantia pelo período solicitado em cada item conforme sua exigência;

d) responsabilizar-se por todas as despesas oriundas das entregas bem como de suas eventuais e trocas durante a garantia;

e) enviar por *e-mail* o arquivo XML/PDF oriundo da emissão do DANFE para os endereços eletrônicos de cada Órgão Participante;

f) manter as condições de habilitação e qualificação exigidas na licitação e comprovar a regularidade fiscal e trabalhista junto ao Órgão Participante;

g) acusar o recebimento das Autorizações de Fornecimento, bem como de qualquer outra notificação enviadas por meio eletrônico, no prazo máximo de 24 (vinte e quatro) horas. Se o prazo final deste item recair em final de semana ou feriado, será prorrogado ao próximo dia útil.

h) emitir Nota Fiscal dos produtos e/ou serviços realizados, discriminando-os individual e pormenorizadamente, especificando quantitativos, marcas e modelos.

i) a nota fiscal emitida deverá conter destacado o valor de todos os Tributos passível de retenção pelo Órgão Participantes, nos termos da legislação em vigor, especialmente o IRRF, nos termos da IN RFB 1.234/2012.

5.2 Será de responsabilidade do Órgão Participante:

a) pagamento dos produtos contratados, nos prazos previstos;

b) fiscalização dos fornecimentos, relatando problemas e circunstâncias para facilitação dos

serviços;

c) indicar prepostos para contato com os responsáveis da fornecedora;

d) cumprir as obrigações previstas no Edital e nesta Ata e exigir o cumprimento das obrigações previstas para a Contratada;

e) demais disposições contidas nesta ata e na lei.

## 6. CLÁUSULA SEXTA – DAS SANÇÕES ADMINISTRATIVAS

6.1 Nas hipóteses de inexecução total ou parcial do Contrato e das obrigações nele assumidas, poderá o Órgão Gerenciador aplicar ao fornecedor em relação as contratações do Órgão Participante as seguintes sanções:

a) advertência;

b) impedimento de licitar e contratar com o CIMLAGO, bem como com qualquer um dos municípios consorciados, por prazo não superior a 03 (três) anos.

c) por atraso superior a 5 (cinco) dias da entrega do objeto, fica o FORNECEDOR constituído em mora, sujeito a multa de 0,5% (meio por cento) por dia de atraso, incidente sobre o valor total do contrato a ser calculado desde o 6° (sexto) dia de atraso até o efetivo cumprimento da obrigação limitado a 30 (trinta) dias;

d) em caso de inexecução parcial ou de qualquer outra irregularidade do objeto poderá ser aplicada multa de

10% (dez por cento) calculada sobre o valor do contrato, ou proporcional por cada descumprimento;

e) transcorridos 30 (trinta) dias do prazo de entrega estabelecido no contrato, será considerado rescindido o Contrato, cancelado o Registro de Preços e aplicado a multa de 15% (quinze por cento) por inexecução total, calculada sobre o valor da contratação;

f) dependendo do descumprimento, se gerar algum prejuízo ao CIMLAGO ou a qualquer um dos municípios consorciados, poderá ser requerido do Fornecedor o valor de perdas e danos conforme caso, após Processo Administrativo de reconhecimento da responsabilidade.

g) declaração de inidoneidade, nos termos do art. 156, IV e §§ 5º e 6º, da Lei Federal nº 14.133, de 2021.

6.2 O licitante ou contratado também terá responsabilidade administrativa pelas infrações previstas no art. 155, da Lei Federal nº 14.133, de 2021.

6.3 A aplicação das sanções ao responsável pelas infrações administrativas seguirá as disposições previstas nos art. 156 a 163, da Lei Federal nº 14.133, de 2021.

6.4 Na hipótese de aplicação de penalidade de multa, após os procedimentos legais, será emitida notificação de cobrança ao licitante, que deverá fazer o recolhimento do valor no prazo estabelecido na decisão do processo administrativo, sob pena de cobrança judicial.

## 7. CLÁUSULA SÉTIMA – DA RESCISÃO CONTRATUAL

7.1 As causas de rescisão contratual estão estabelecidas no artigo 137, de acordo com as disposições do art. 138 e 139, todos da Lei Federal nº 14.133, de 2021.

## 8. CLÁUSULA OITAVA – DAS ALTERAÇÕES DA ATA DE REGISTRO DE PREÇOS

8.1 A Ata de Registro de Preços poderá sofrer alterações, obedecidas às disposições contidas nas **Resoluções 004/2024 e 006/2024,** do CIMLAGO ou outra que vier a substituir.

8.1.1 O preço registrado poderá ser revisto em decorrência de eventual redução daqueles praticados no mercado, ou de fato que eleve o custo dos serviços ou bens registrados, cabendo ao Órgão Gerenciador da Ata de Registro de Preços promover as necessárias negociações junto aos fornecedores.

8.1.2 Quando o preço inicialmente registrado, por motivo superveniente, tornar-se superior ao preço praticado no mercado o Órgão Gerenciador deverá:

I. Convocar o fornecedor visando a negociação para redução de preços e sua adequação ao praticado pelo mercado;

II. Frustrada a negociação, o fornecedor será liberado do compromisso assumido sem aplicação de penalidade; e

III. Convocar os demais fornecedores visando igual oportunidade de negociação.

8.1.3 Quando o preço de mercado se tornar superior aos preços registrados e o fornecedor, mediante requerimento devidamente comprovado, não puder cumprir o compromisso, o Órgão Gerenciador poderá:

I. Liberar o fornecedor do compromisso assumido, caso a comunicação ocorra antes do pedido de fornecimento, e sem aplicação da penalidade se confirmada a veracidade dos motivos e comprovantes apresentados; e

II. Convocar os demais fornecedores para assegurar igual oportunidade de negociação.

8.1.4 Não havendo êxito nas negociações, o Órgão Gerenciador deverá proceder à revogação da Ata de Registro de Preços, adotando as medidas cabíveis para obtenção da contratação mais vantajosa.

8.2 É possível realizar aumento nos quantitativos fixados pela Ata de Registro de Preços, até uma vez a quantidade registrada inicialmente, desde que com aceitação expressa do fornecedor, formalizada mediante apostilamento, quando caracterizadas circunstâncias supervenientes, devidamente demonstradas nos autos do procedimento administrativo em que tramitar a alteração, que indiquem que as estimativas inicialmente previstas neste edital serão insuficientes para atender a demanda durante o prazo de vigência.

## 9. CLÁUSULA NONA – DO CANCELAMENTO DO REGISTRO DE PREÇOS

9.1 O FORNECEDOR terá seu registro cancelado quando:

I Descumprir as condições da Ata de Registro de Preços;

II Não retirar a nota de empenho e ou autorização de fornecimento de compra no prazo estabelecido pela Administração, sem justificativa aceitável;

III Não aceitar reduzir o seu preço registrado, na hipótese de este se tornar superior àqueles praticados no mercado;

IV Tiver presentes razões de interesse público;

V Sofrer sanções impeditivas previstas em lei;

VI For declarado inidôneo ou impedido de licitar ou contratar com o CIMLAGO ou com qualquer um dos Municípios Consorciados nos termos do artigo 156, inciso IV, da Lei Federal nº. 14.133, de 2021.

9.2 O cancelamento do registro de preços, nas hipóteses previstas, assegurados o contraditório e a ampla defesa, serão formalizados por despacho da autoridade competente do Órgão Gerenciador.

9.3 O cancelamento do registro de preços poderá ocorrer por fato superveniente, decorrente de caso fortuito ou força maior, que prejudique o cumprimento da ata, devidamente comprovados e justificados:

I. Por razão de interesse público; ou

II. A pedido do fornecedor.

## 10. CLÁUSULA DÉCIMA – DA DOTAÇÃO ORÇAMENTÁRIA

10.1 As despesas decorrentes da aquisição, objeto da presente Ata de Registro de Preços correrão a conta de dotação específica do orçamento do exercício de 2024 e seguintes de cada Órgão Participante.

10.2 O Órgão Participante quando da contratação/empenhamento especificará a classificação orçamentária.

## 11. CLÁUSULA DÉCIMA PRIMEIRA – DA VINCULAÇÃO AO PROCESSO LICITATÓRIO

11.1 A presente **Ata de Registro de Preços está vinculada ao Processo Administrativo Licitatório Eletrônico n° 016/2024, Pregão, na Forma Eletrônica Nº 016/2024, Registro de Preços**, realizado pelo CIMLAGO, Órgão Gerenciador.

## 12. CLÁUSULA DÉCIMA SEGUNDA – DA VALIDADE E DA VIGÊNCIA

12.1 O prazo de validade da Ata de Registro de Preços será de 12 (doze) meses a contar da data da sua assinatura.

12.2 O prazo de validade da Ata de Registro de Preços poderá ser prorrogado, por igual período, desde que comprovado o preço vantajoso, nos termos do art. 84, da Lei Federal nº 14.133, de 2021.

12.2.1 Em caso de prorrogação da vigência da Ata de Registro de Preços, as quantidades inicialmente registradas serão renovadas, na sua totalidade, independentemente do quantitativo utilizado no período de vigência, não sendo possível cumular com as quantidades não utilizadas.

12.3 O prazo de vigência para a execução dos contratos (autorizações de fornecimento) decorrentes desta Ata de Registro de Preços será idêntico ao prazo de entrega do bem.

12.3.1 O prazo de vigência do contrato (autorização de fornecimento) será automaticamente prorrogado quando seu objeto não for concluído no prazo de entrega.

12.3.2 O prazo de vigência do contrato não se confunde com o prazo de entrega do bem, e a aceitação de recebimento posterior do(s) item(ns) não se configura como novo prazo de entrega.

12.3.3 Caso a entrega deixar de ser cumprida ou ocorrer fora do prazo previsto em decorrência de culpa do contratado, ele será constituído em mora, sendo-lhe aplicáveis as respectivas sanções administrativas, e o Órgão Gerenciador poderá optar pela extinção do

contrato e, nesse caso, adotará as medidas admitidas em lei para a continuidade da execução contratual.

## 13. CLÁUSULA DÉCIMA TERCEIRA – DAS DISPOSIÇÕES GERAIS

13.1 O Registro de Preços objeto desta Ata e a sua assinatura pelas partes não gera ao (Órgão Gerenciador (CIMLAGO) ou para os Órgãos Participantes a obrigação de solicitar os fornecimentos que dele poderão advir independentemente da sua estimativa de consumo).

13.2 Observados os critérios e condições estabelecidas no Edital e o preço registrado, o Órgão Participante poderá comprar de mais de um fornecedor registrado, segundo a ordem de classificação, desde que razões de interesse público justifiquem e que o primeiro classificado não possua capacidade de fornecimento compatível com o solicitado pelo Órgão Participante.

13.3 A existência de preços registrados não obriga o Órgão Gerenciador ou os Órgãos Participantes a firmar as contratações que deles poderão advir, facultando-se a realização de licitação específica para a aquisição pretendida, sendo assegurado ao beneficiário do registro a preferência de fornecimento em igualdade de condições.

13.4 O FORNECEDOR signatário desta Ata, cujo preço é registrado, declara estar ciente das suas obrigações para com o Órgão Gerenciador e os Órgãos Participantes, nos termos do Edital da respectiva Licitação e da sua Proposta, que passam a fazer parte integrante da presente Ata de Registro de Preços e a reger as relações entre as partes, para todos os fins.

## 14. CLÁUSULA DÉCIMA QUARTA – DO TRATAMENTO DE DADOS PESSOAIS

14.1 As Partes comprometem-se a observar o disposto na Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados LGPD) quanto ao tratamento de dados pessoais e dados pessoais sensíveis aos quais tiverem acesso em decorrência deste contrato, compatibilizando-a com o que estabelece a Lei Federal nº 12.527 (Lei de Acesso à Informação LAI), tendo em vista o caráter público desta contratação.

14.2 As Partes terão acesso a dados pessoais dos respectivos representantes, tais como número e cópia de documentos de identificação (Cadastro de Pessoa Física e Registro Geral) e endereços eletrônico e residencial, e outros dados que sejam imprescindíveis para a formação e execução deste contrato, sendo-lhes vedado utilizá-los para finalidade distinta daquela do objeto da contratação, sob pena de responsabilização administrativa, civil e criminal.

14.3 Considerando o caráter público desta contratação, o compartilhamento de dados observará ao disposto no Capítulo IV da LGPD.

14.4 A CONTRATADA declara adotar medidas de segurança eficazes para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas, comprometendo-se a comunicar à CONTRATANTE, no prazo de 48 (quarenta e oito horas), a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares e responsabilizando-se pelos danos de qualquer natureza ocorridos em caso de violação à legislação de proteção de dados pessoais.

## 15. CLÁUSULA DÉCIMA QUINTA – ANTICORRUPÇÃO

15.1 As partes declaram conhecer as normas de prevenção à corrupção prevista na legislação brasileira, dentre elas, a Lei de Improbidade Administrativa (Lei Federal nº 8.429/1992), a Lei Federal nº 12.846/2013 e seus regulamentos, e se comprometem que, para a execução deste contrato nenhuma das partes poderá oferecer, dar ou se comprometer a dar, a quem quer que seja, aceitar ou se comprometer a aceitar, de quem quer que seja, tanto por conta própria quanto por intermédio de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou benefícios indevidos de qualquer espécie, de modo fraudulento que constituam prática ilegal ou de corrupção, bem como de manipular ou fraudar o equilíbrio econômico financeiro do presente contrato, seja de forma direta ou indireta quanto ao objeto deste contrato, devendo garantir, ainda, que seus prepostos, administradores e colaboradores ajam da mesma forma.

## 16. CLÁUSULA DÉCIMA SEXTA – TABELA DE REGISTRO DE PREÇOS

16.1 – Tabela de itens e preços registrados:

| Item | Unid. | Descrição | Qtde | Valor Unit. | Valor Total |
|---|---|---|---|---|---|
| .. | .. | .. | .. | | .. |

## 17. CLÁUSULA DÉCIMA SÉTIMA – DA ADESÃO A ATA DE REGISTRO DE PREÇOS

17.1 Órgãos Não Participantes desde que devidamente justificada a vantagem, a Ata de Registro de Preços, durante sua vigência, poderá ser utilizada por qualquer órgão ou entidade da administração pública dos Entes da Federação que não aderiram ao Projeto de Licitações Compartilhadas do CIMLAGO e/ou não tenham participado do certame licitatório e/ou não estejam previstos no edital como órgãos participantes, mediante anuência do Órgão Gerenciador.

17.2 Os órgãos e entidades que não participaram do registro de preços, quando desejarem fazer uso da Ata de Registro de Preços, deverão consultar o Órgão Gerenciador da ata para manifestação sobre a possibilidade de adesão.

17.3 A manifestação do Órgão Gerenciador de que trata o item 17.2 fica condicionada à realização de estudo, pelos órgãos e pelas entidades que não participaram do registro de preços, que demonstre o ganho de eficiência, a viabilidade e a economicidade para a administração pública da utilização da Ata de Registro de Preços, inclusive em situações de provável desabastecimento ou descontinuidade de serviço público.

17.4 Caberá ao fornecedor beneficiário da Ata de Registro de Preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento decorrente de adesão, desde que não prejudique as obrigações presentes e futuras decorrentes da ata, assumidas com o Órgão Gerenciador e Órgãos Participantes.

17.5 As aquisições ou as contratações adicionais de que trata este artigo não poderão exceder, por órgão ou entidade, a 50% (cinquenta por cento) dos quantitativos dos itens do instrumento convocatório e registrados na Ata de Registro de Preços para o Órgão Gerenciador e para os Órgãos Participantes.

17.6 O quantitativo decorrente das adesões à Ata de Registro de Preços não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na Ata de Registro de Preços para o Órgão Gerenciador e para os Órgãos Participantes, independentemente do número de órgãos não participantes que aderirem.

17.7 Após a autorização do Órgão Gerenciador da utilização da Ata de Registro de Preços, o órgão não participante deverá efetivar a aquisição ou contratação solicitada em até 90 (noventa) dias, podendo o mesmo ser prorrogado por igual período desde que devidamente justificado, observado o prazo de vigência da ata

## 18. CLÁUSULA DÉCIMA OITAVA – DO FORO

18.1 É competente o foro da Comarca da Cidade de Alfenas/MG, para dirimir quaisquer dúvidas, porventura, oriundas da presente Ata de Registro de Preços.

## 19. CLÁUSULA DÉCIMA NONA – DAS NORMAS E PRECEITOS COMPLEMENTARES

19.1 Aplicam-se à execução desta Ata e aos casos omissos as normas da Lei Federal nº 14.133, de 2021 e alterações posteriores, os preceitos do direito público, os princípios da teoria geral dos Contratos e as disposições do direito privado.

E por estarem justas e compromissadas, as partes assinam a presente Ata de Registro de Preços.

Alfenas (MG), ..../...../ 2024

| Pelo Órgão Gerenciador: | Pelo Fornecedor: |
| --- | --- |
| Consórcio Intermunicipal Multifinalitário Dos Municípios Do Lago De Furnas – CIMLAGO<br><br>Luiza Maria Lima Menezes<br><br>Presidente | Razão Social:<br><br>CNPJ:<br><br>Representante Legal |
| Testemunhas: | |
| Nome: | Nome |
| CPF: | CPF: |

ANEXO XII – MINUTA DE CONTRATO ADMINISTRATIVO LICITATÓRIO

CONTRATO ADMINISTRATIVO LICITATÓRIO N° ___/2024, QUE FAZEM ENTREI SI O CONSÓRCIO INTERMUNICIPAL MULTIFINALITÁRIO DOS MUNICÍPIOS DO LAGO DE FURNAS – CIMLAGO E A EMPRESA _____.

A Prefeitura Municipal de _____, com sede no (a) _____, na cidade de _____ /Estado _____, inscrito(a) no CNPJ sob o nº _____, neste ato representado(a) por seu (ua) Prefeito (a) Municipal, senhor (a) _____, inscrito na Cédula de Identidade _____, CPF sob o n° _____, doravante denominado **CONTRATANTE**, e o(a) _____, inscrito(a) no CNPJ/MF sob o nº _____, sediado(a) na _____, doravante designado **CONTRATADO**, neste ato representado(a) pelo senhor (a) _____, inscrito na Cédula de Identidade _____, CPF sob o n° _____, tendo em vista o que consta **no Processo Administrativo Licitatório nº 016/2024** 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, na forma Eletrônica n. 016/2024**, referente a licitação compartilhada do Consórcio Intermunicipal Multifinalitário Dos Municípios Do Lago De Furnas CIMLAGO, mediante as cláusulas e condições a seguir enunciadas.

## 1. CLÁUSULA PRIMEIRA – OBJETO

1.1. O Objeto do presente instrumento é contratação de infraestrutura como serviço, abrangendo soluções de armazenamento inteligente, proteção e armazenamento de dados, soluções de redes, proteção de perímetro, endpoint e gerenciamento de vulnerabilidades, com a finalidade de proporcionar ampla capacidade de atendimento aos usuários dos sistemas, incluindo serviços de instalação, configuração, transferência de conhecimento técnico e gerenciamento do ambiente, destinados a suprir futuras demandas, conforme especificações e condições estabelecidas no Anexo I e demais disposições do Edital, para atender os municípios consorciados ao Consórcio Intermunicipal Multifinalitário dos Municípios do Lago de Furnas – CIMLAGOf, para uso da _____.

1.2. Tabela de itens, quantitativos e valores da contratação.

| Item | Unid. | Descrição | Qtde | Valor Unit. | Valor Total |
|---|---|---|---|---|---|
| .. | .. | .. | .. | | .. |

1.3. 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.

1.4. Vinculam a esta contratação, a licitação compartilhada do CIMLAGO, independentemente de transição:

1.4.1. O Termo de Referência;

1.4.2. O Edital da Licitação

1.4.3. A Proposta do Contratado

1.4.4. Eventuais anexos dos documentos supracitados.

## 2. CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1 O prazo de vigência da contratação é de (dia ___), (mês___) de 2024 até (dia___), (mês___) de 2024.

2.2 O presente contrato poderá ser prorrogável na forma dos artigos 106 e 107 da Lei n° 14.133/2021, quando for o caso.

2.3 A prorrogação de que trata o item 2.2. é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o contratado.

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

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

## 3. CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS

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, edital e seus anexos.

## 4. CLÁUSULA QUARTA – SUBCONTRATAÇÃO

4.1. Será admitida a subcontratação do objeto licitatório, desde que observados os limites estabelecidos em lei.

## 5. CLÁUSULA QUINTA – PAGAMENTO

5.1. O prazo para pagamento ao contratado e demais condições a ele referentes encontram-se definidos no Termo de Referência, edital e seus anexos.

## 6. CLÁUSULA SEXTA – REAJUSTE

6.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, em __/__/__ *(DD/MM/AAAA)*.

6.2. Após o interregno de um ano, e independentemente de pedido do contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo CONTRATANTE, do índice que será definido e formalizado no ato da contratação pelos órgãos participantes em contrato formal assinado pelas partes, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

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

6.4. 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).

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

6.6. 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.

6.7. 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.

6.8. O reajuste será realizado por apostilamento.

## 7. CLÁUSULA SÉTIMA – OBRIGAÇÕES DO CONTRATANTE

7.1. São obrigações do CONTRATANTE:

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

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

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

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

7.6. Efetuar o pagamento ao Contratado do valor correspondente ao fornecimento do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência.

7.7. Aplicar ao Contratado as sanções previstas na lei e neste Contrato;

7.8. 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.

7.9. A Administração terá o prazo de 40 (quarenta) dias, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.

7.10. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo contratado no prazo máximo de 40 (quarenta) dias.

7.11. 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.

## 8. CLÁUSULA OITAVA OBRIGAÇÕES DO CONTRATADO

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

8.3. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

8.4. Comunicar ao CONTRATANTE, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

8.5. Atender às determinações regulares emitidas pelo fiscal ou gestor do contrato ou autoridade superior (art. 137, II, da Lei n.º 14.133, de 2021) e prestar todo esclarecimento ou informação por eles solicitados;

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

8.7. 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;

8.8. Entregar ao setor responsável pela fiscalização do contrato, junto com a Nota Fiscal para fins de pagamento, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda Estadual ou Distrital do domicílio ou sede do contratado; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT;

8.9. Responsabilizar-se pelo cumprimento de todas as obrigações trabalhistas, previdenciárias, 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;

8.10. Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local da execução do objeto contratual.

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

8.12. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação;

8.13. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação (art. 116, da Lei n.º 14.133, de 2021);

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

8.15. 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.

8.16. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do CONTRATANTE;

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

8.18. Orientar e treinar seus empregados sobre os deveres previstos na Lei nº 13.709, de 14 de agosto de 2018, adotando medidas eficazes para proteção de dados pessoais a que tenha acesso por força da execução deste contrato, quando for o caso;

8.19. 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, quando for o caso.

8.20. 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, quando for o caso.

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

## 9. CLÁUSULA NONA – GARANTIA DE EXECUÇÃO

9.1. Não haverá exigência de garantia contratual da execução deste objeto.

## 10. CLÁUSULA DÉCIMA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

10.1. Comete infração administrativa, nos termos da Lei Federal n° 14.133/2021, o contratado que:

10.1.1. der causa à inexecução parcial do contrato;

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

10.1.3. der causa à inexecução total do contrato;

10.1.4. ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

10.1.5. apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

10.1.6. praticar ato fraudulento na execução do contrato;

10.1.7. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

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

10.2. Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:

10.2.1. advertência;

10.2.2. impedimento de licitar e contratar com o CIMLAGO, bem como com qualquer um dos municípios consorciados, por prazo não superior a 03 (três) anos.

10.2.3. por atraso superior a 5 (cinco) dias da entrega do objeto, fica o FORNECEDOR constituído em mora, sujeito a multa de 0,5% (meio por cento) por dia de atraso, incidente sobre o valor total do contrato a ser calculado desde o 6° (sexto) dia de atraso até o efetivo

cumprimento da obrigação limitado a **30 (trinta) dias**;

10.2.4. em caso de inexecução parcial ou de qualquer outra irregularidade do objeto poderá ser aplicada multa de

**10% (dez por cento)** calculada sobre o valor do contrato, ou proporcional por cada descumprimento;

10.2.5. transcorridos **30 (trinta) dias** do prazo de entrega estabelecido no contrato, será considerado rescindido o Contrato, cancelado o Registro de Preços e aplicado a multa de **15% (quinze por cento)** por inexecução total, calculada sobre o valor da contratação;

10.2.6. dependendo do descumprimento, se gerar algum prejuízo ao CIMLAGO ou a qualquer um dos municípios consorciados, poderá ser requerido do Fornecedor o valor de perdas e danos conforme caso, após Processo Administrativo de reconhecimento da responsabilidade.

10.2.7. declaração de inidoneidade, nos termos do art. 156, IV e §§ 5º e 6º, da Lei Federal nº 14.133, de 2021.

10.3. O licitante ou contratado também terá responsabilidade administrativa pelas infrações previstas no art. 155, da Lei Federal nº 14.133, de 2021.

10.4. A aplicação das sanções ao responsável pelas infrações administrativas seguirá as disposições previstas nos art. 156 a 163, da Lei Federal nº 14.133, de 2021.

10.5. Na hipótese de aplicação de penalidade de multa, após os procedimentos legais, será emitida notificação de cobrança ao licitante, que deverá fazer o recolhimento do valor no prazo estabelecido na decisão do processo administrativo, sob pena de cobrança judicial.

## 11. CLÁUSULA DÉCIMA PRIMEIRA – DOTAÇÃO ORÇAMENTÁRIA

11.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral do Município deste exercício, na dotação abaixo discriminada:

11.2. Rubrica orçamentaria: _____.

A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

## 12. CLÁUSULA DÉCIMA SEGUNDA – DOS CASOS OMISSOS

Os casos omissos serão decididos pelo CONTRATANTE, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas 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.

## 13. CLÁUSULA DÉCIMA TERCEIRA – ALTERAÇÕES

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

13.2. 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.

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

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

## 14. CLÁUSULA DÉCIMA QUARTA – FORO

14.1. Fica eleito o Foro da Comarca de _____/MG para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não puderem ser compostos pela conciliação, conforme art. 92, §1º, da Lei nº 14.133/21

Alfenas (MG), ..../...../ 2024

**Pelo CONTRATANTE:**

_____

**Prefeitura Municipal de _____**

Nome _____

Prefeito (a)

**Pelo Fornecedor:**

_____

Razão Social:

CNPJ:

Representante Legal

**Testemunhas:**

Nome:

CPF:

Nome

CPF: