Belo Horizonte, 09 de dezembro de 2024.

Edital Pregão de Serviço(Lei14133) PMMG/DTS/CSA-TIC LICITAÇÕES Nº 103463666/2024

EDITAL PREGÃO DE SERVIÇO(LEI14133)

EDITAL DE LICITAÇÃO PREGÃO ELETRÔNICO

PREGÃO ELETRÔNICO Nº 274/2024	
PROCESSO DE COMPRA:	**1250071 - 274/2024**
CONTRATANTE:	**Polícia Militar de Minas Gerais**
OBJETO:	**Solução de Tecnologia Hiperconvergente**
VALOR ESTIMADO:	**Orçamento sigiloso**
CRITÉRIO DE JULGAMENTO:	**MENOR PREÇO POR LOTE**
MODO DE DISPUTA:	**ABERTO E FECHADO**
EXCLUSIVIDADE ME/EPP/EQUIPARADAS:	**Licitação com participação ampla (sem reserva de lotes para ME e EPP), conforme disposto no Anexo I, Termo de Referência.**
LOCAL: Portal de Compras do Estado de Minas Gerais - http://compras.mg.gov.br/	
DATA DA ABERTURA DA SESSÃO	**HORÁRIO DA ABERTURA DA SESSÃO**
07/01/2025	09:00 horas

SUMÁRIO

Sumário

1. PREÂMBULO

Torna-se público que o ESTADO DE MINAS GERAIS, por intermédio da Polícia Militar de Minas Gerais, representada pelo Centro de Aquisições e Suprimentos - TIC realizará licitação na modalidade pregão eletrônico do tipo menor preço, no modo de disputa aberto e fechado, regime de contratação de serviço e fornecimento de bens, em sessão pública, por meio do site www.compras.mg.gov.br, visando a **contratação/aquisição de Solução de Tecnologia Hiperconvergente,** nos termos da Lei Federal n° 14.133, de 1º de abril de 2021 e do Decreto n° 48.723, de 24 de novembro de 2023, e demais legislações aplicáveis.

2. DO OBJETO

2.1. A presente licitação tem por objeto a **contratação/aquisição de Solução de Tecnologia Hiperconvergente,** conforme especificações, quantitativos e condições constantes neste Edital e dos seus anexos.

2.2. Havendo mais de um lote, faculta-se ao fornecedor a participação em quantos forem de seu interesse. Ressalta-se que ao optar por participar do lote, a proposta deverá contemplar todos os itens que o compõe.

2.3. Em caso de divergência entre as especificações do objeto descritas no Portal de Compras e as especificações técnicas constantes no Anexo I - Termo de Referência, o licitante deverá obedecer a este último.

3. DO PEDIDO DE ESCLARECIMENTOS E DA IMPUGNAÇÃO DO ATO CONVOCATÓRIO

3.1. Os pedidos de esclarecimentos e os registros de impugnações referentes a este processo licitatório deverão ser enviados ao Pregoeiro até 03 (três) dias úteis anteriores à data fixada para abertura da sessão pública, exclusivamente por meio eletrônico, no Portal de Compras do Estado de Minas Gerais.

3.2. O pedido de esclarecimentos ou registro de impugnação pode ser feito por qualquer pessoa no Portal de Compras/MG na página da licitação, em campo próprio (acesso via botão “Esclarecimentos/Impugnação”).

3.2.1. Nos pedidos de esclarecimentos ou registros de impugnação os interessados deverão se identificar (CNPJ, Razão Social e nome do representante que pediu esclarecimentos, se pessoa jurídica, e CPF e nome do interessado para pessoa física) e disponibilizar as informações para contato (telefone e e-mail).

3.2.2. Podem ser inseridos arquivos anexos com informações e documentações pertinentes as solicitações.

3.2.3. Após o envio da solicitação, as informações não poderão ser mais alteradas, ficando o pedido registrado com número de entrada, tipo (esclarecimento ou impugnação), data de envio e sua situação.

3.2.4. A resposta ao pedido de esclarecimento ou ao registro de impugnação também será disponibilizada via sistema. O solicitante receberá um e-mail de notificação e a situação da solicitação alterar-se-á para “concluída”.

3.3. O Pregoeiro responderá no prazo de 03 (três) dias úteis, contados da data de recebimento, limitado ao último dia útil anterior à data da abertura do certame, e poderá requisitar subsídios formais aos responsáveis pela elaboração do edital de licitação e dos anexos.

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

3.4.1. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo Pregoeiro, nos autos do processo de licitação, nos termos do art. 14, §2º do Decreto 48.723/2023.

3.5. As respostas aos pedidos de impugnações e esclarecimentos aderem a este Edital tal como se dele fizessem parte, vinculando a Administração e os licitantes.

3.6. Acolhida a impugnação, será definida e publicada nova data para a realização do certame, observados os prazos fixados no art. 55 da Lei Federal nº 14.133/ 2021 e do art. 15 do Decreto 48.723/2023.

3.7. Qualquer modificação no Edital exige divulgação pelo mesmo instrumento de publicação em que se deu o texto original, reabrindo-se o prazo inicialmente estabelecido, exceto quando, inquestionavelmente, a alteração não afetar a formulação das propostas.

3.8. As denúncias, petições e impugnações anônimas ou não fundamentadas não serão analisadas e serão arquivadas pela autoridade competente.

3.9. A não impugnação do edital, na forma e tempo definidos nesse item, acarreta a decadência do direito de discutir, na esfera administrativa, as regras do certame.

4. DAS CONDIÇÕES DE PARTICIPAÇÃO

4.1. A participação no presente Edital se dará exclusivamente por meio do Portal de Compras do Estado de Minas Gerais.

4.1.1. As orientações para participação neste Edital são apresentadas no Manual da licitação pelos critérios de julgamento de menor preço e maior desconto – Decreto 48.723/2023, versão Fornecedor.

4.2. Será concedido tratamento favorecido para as microempresas, empresas de pequeno porte e demais licitantes enquadrados como beneficiários indicados no caput do art. 3º do Decreto nº 47.437/2018, nos limites previstos na Lei Complementar nº 123/2006 e no mencionado Decreto 47.437/2018.

4.3. A obtenção do benefício a que se refere o subitem anterior:

4.3.1. não se aplica no caso de licitação para aquisição de bens ou contratações de serviços em geral, ao item cujo valor estimado for superior à receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte.

4.3.2. fica limitada às microempresas e às empresas de pequeno porte que, no ano-calendário de realização do procedimento, ainda não tenham celebrado contratos com a Administração Pública, cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte.

4.3.3. nas contratações com prazo de vigência superior a 1 (um) ano, deverá ser considerado o valor anual do contrato na aplicação dos limites previstos nos subitens 4.3.1. e 4.3.2.

4.4. Para fins do disposto neste edital, o enquadramento dos beneficiários indicados no caput do art. 3º do Decreto Estadual nº 47.437, de 26 de junho de 2018 se dará da seguinte forma:

4.4.1. microempresa ou empresa de pequeno porte, conforme definido nos incisos I e II do caput § 4º do art. 3º da Lei Complementar Federal nº 123, de 14 de dezembro de 2006;

4.4.2. agricultor familiar, conforme definido na Lei Federal nº 11.326, de 24 de julho de 2006;

4.4.3. produtor rural pessoa física, conforme disposto na Lei Federal nº 8.212, de 24 de julho de 1991;

4.4.4. microempreendedor individual, conforme definido no § 1º do art. 18-A da Lei Complementar Federal nº 123, de 14 de dezembro de 2006;

4.4.5. sociedade cooperativa, conforme definido no art. 34 da Lei Federal nº 11.488, de 15 de junho de 2007, e no art. 4º da Lei Federal nº 5.764, de 16 de dezembro de 1971.

4.5. **Poderão participar** desta licitação os fornecedores cujo ramo de atividade seja compatível com o objeto desta licitação, e que estejam regularmente credenciados no Cadastro Geral de Fornecedores – CAGEF do Estado de Minas Gerais, nos termos do Decreto Estadual nº 47.524, de 6 de novembro de 2018 e Resolução SEPLAG nº 93, de 28 de novembro de 2018.

4.5.1. O credenciamento no CAGEF deve ser realizado no prazo mínimo de 02 (dois) dias úteis antes da data da abertura da COTEP, por meio do site www.compras.mg.gov.br - Opção Cadastro de Fornecedores.

4.5.2. Cada fornecedor deverá credenciar, no mínimo, um representante para atuar em seu nome no sistema, sendo vedado a qualquer pessoa, física ou jurídica, representar mais de um licitante no presente Edital.

4.5.3. O representante receberá uma senha eletrônica de acesso, de caráter pessoal e intransferível, ficando excluída da responsabilidade do provedor ou do órgão/entidade promotor do Edital por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros não autorizados.

4.5.4. É dever do responsável legal conferir a exatidão dos seus dados cadastrais no CAGEF e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

4.5.5. A inscrição junto ao provedor do sistema implica a presunção da capacidade técnica do licitante e do seu representante para realização das transações inerentes ao Edital.

4.5.6. O licitante se responsabiliza:

4.5.6.1. pelas transações efetuadas em seu nome, assumindo como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante;

4.5.6.2. pelo acompanhamento das operações no sistema, admitindo ônus decorrente da perda do negócio diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

4.5.7. Informações complementares a respeito do credenciamento podem ser obtidas no site www.compras.mg.gov.br ou pela Central de Atendimento aos Fornecedores, via e- mail: cadastro.fornecedores@planejamento.mg.gov.br, com horário de atendimento de segunda a sexta-feira, das 08:00h às 16:00h.

4.6. O fornecedor que desejar obter os benefícios previstos no Capítulo V da Lei Complementar Federal nº 123/2006, disciplinados no Decreto Estadual nº. 47.437, de 2018 e pela Resolução Conjunta SEPLAG/SEF/JUCEMG nº 9.576, de 6 de julho de 2016, deverá comprovar a condição de beneficiário no momento do seu credenciamento ou quando da atualização de seus dados cadastrais no Cadastro Geral de Fornecedores – CAGEF, desde que ocorram em momento anterior ao cadastramento da proposta comercial.

4.6.1. Não havendo comprovação, no CAGEF, da condição de beneficiário até o momento do registro de proposta, o fornecedor não fará jus aos benefícios listados no Decreto Estadual nº 47.437, de 26 de junho de 2018.

4.7. N**ão poderão participar deste Edital as empresas que**:

4.7.1. Não atendam às condições deste Edital e seus anexos;

4.7.2. Enquadrem-se como empresa estrangeira que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;

4.7.3. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição (Acórdão nº 746/2014-TCU-Plenário).

4.7.4. Que se enquadrem nas seguintes situações:

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

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

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

4.7.4.3. Pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta, conforme legislação vigente;

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

4.7.4.4. Aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

4.7.4.5. Empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

4.7.4.6. Empresas que tenham como proprietários controladores ou diretores membros dos poderes legislativos da União, Estados ou Municípios ou que nelas exerçam funções remuneradas, conforme art. 54, II, “a”, c/c art. 29, IX, ambos da Constituição da República;

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

5. DA APRESENTAÇÃO DA PROPOSTA

5.1. Após a divulgação do edital de licitação, os licitantes encaminharão, **exclusivamente por meio do Portal de Compras MG, a proposta com o preço/menor preço**, até a data e o horário estabelecidos para abertura da sessão pública quando, então, encerrar-se-á automaticamente a etapa de envio dessa documentação, informando, obrigatoriamente no sistema:

5.1.1. **a marca e modelo; exceto no item de serviço**

5.1.2. o valor total do lote.

5.2. Os licitantes poderão retirar ou substituir a proposta anteriormente inserida no sistema até a abertura da sessão pública.

5.3. Nesta etapa não haverá ordem de classificação, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.

5.4. Os preços ofertados, tanto na fase do lançamento da proposta no sistema, quanto na sessão de lances, serão de exclusiva responsabilidade do fornecedor, e deverão:

5.4.1. ser apresentados em moeda corrente nacional, em algarismos com duas casas decimais após a vírgula.

5.4.2. incluir todos os tributos, encargos sociais, frete até o destino e quaisquer outros ônus que porventura possam recair sobre o fornecimento do objeto, os quais ficarão a cargo única e exclusivamente do fornecedor, inclusive os custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos eventuais termos de ajustamento de conduta vigentes na data de entrega das propostas.

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

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

5.6. A apresentação das propostas implica obrigatoriedade no cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de cumprir o objeto nos seus termos, **bem como de fornecer os aplicativos em quantidades e qualidades adequadas à perfeita execução contratual**, promovendo, quando requerido, sua substituição, quando for o caso.

5.7. **O prazo de validade da proposta será de 90 (noventa) dias contados** da data de abertura da sessão pública estabelecida no preâmbulo deste Edital e seus anexos.

5.8. No cadastramento da proposta, o fornecedor deverá, também, assinalar em campo próprio do portal de compras, as seguintes declarações:

5.8.1. que manifesta ciência em relação ao inteiro teor do ato convocatório e dos seus anexos, concorda com suas condições, declara que a sua proposta econômica compreenderá a integralidade dos custos, nos termos do art. 63, §1º, da Lei Federal nº. 14.133, de 2021, para atendimento dos direitos trabalhistas assegurados na Constituição Federal de 1.988, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data da sua entrega em definitivo e atendo aos requisitos de habilitação neles estabelecidos.

5.8.2. que inexiste impedimento à sua habilitação, e comunicará a superveniência de ocorrência impeditiva ao órgão ou entidade Contratante;

5.8.3. que cumpre o disposto no inciso XXXIII do art. 7° da Constituição Federal de 1.988, que proíbe o trabalho noturno, perigoso ou insalubre a menores de dezoito e de qualquer trabalho a menores de dezesseis anos, salvo na condição de aprendiz, a partir de quatorze anos.

5.8.4. que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitação da Previdência Social, previstas em lei nos termos do art. 93 da Lei Federal nº 8.213, de 1991 e em outras normas específicas, conforme previsto no inciso IV do art. 63 da Lei Federal nº. 14.133, de 2021.

5.8.5. que se responsabiliza pelas transações que forem efetuadas no sistema em seu nome, assumindo como firmes e verdadeiras;

5.8.6. No caso de fornecedor beneficiário (ME/EPP/Equiparadas) indicado no caput do art. 3º do Decreto Estadual nº 47.437, de 2018, também deverá ser declarado:

5.8.6.1. que cumpre os requisitos estabelecidos no artigo 3º da Lei Complementar Federal nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus artigos 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021.

5.8.6.2. que caso possua restrição no(s) documento(s) de regularidade fiscal, assume o compromisso de promover a regularização caso venha a formular o lance vencedor, cumprindo plenamente os demais requisitos de habilitação.

5.8.7. No caso de profissionais organizados sob a forma de cooperativa:

5.8.7.1. Que participa da licitação sob a forma de cooperativa e atende ao disposto no art. 16 da Lei nº 14.133 de 1º de abril de 2021.

5.9. A falsidade das declarações mencionadas no item anterior sujeitará o licitante às sanções dispostas no art. 156 da Lei Federal nº 14.133, de 2021, sem prejuízo de outras penalidades aplicáveis.

5.10. **Os fornecedores estabelecidos no Estado de Minas Gerais que usufruem do benefício de isenção do ICMS, conforme dispõe o Decreto Estadual nº 48.589, de 2023, deverão informar na(s) proposta(s) que será(ão) encaminhada(s) no Portal de Compras, o(s) preço(s) resultante(s) da dedução do ICMS, conforme Resolução Conjunta SEPLAG/SEF nº 3.458, de 2003 e alterações.**

5.10.1. **As fases de classificação das propostas, etapa de lances, o julgamento dos preços, a adjudicação e a homologação serão realizadas a partir dos preços dos quais foram deduzidos os valores relativos ao ICMS.**

5.10.2. **O disposto nos subitens 5.11 e 5.11.1 não se aplica aos contribuintes mineiros optantes pelo regime do Simples Nacional.**

5.11. **As informações da(s) proposta(s) comercial(is) encaminhada(s) pelo sistema podem ser alteradas pelo fornecedor até a data e horário marcados para a abertura da sessão.**

6. DA ABERTURA DA SESSÃO E DA ETAPA DE LANCES

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

6.2. Iniciada a fase competitiva, observado o modo de disputa adotado no edital, os licitantes poderão encaminhar lances públicos e sucessivos exclusivamente por meio do Portal de Compras MG.

6.3. O licitante será imediatamente informado do recebimento do seu lance e do valor consignado no registro.

6.4. **O lance deverá ser ofertado pelo valor global**.

6.4.1. O licitante somente poderá oferecer lance de valor inferior em relação ao último lance por ele ofertado, observado o intervalo mínimo de diferença R$ 1.000,00 (um mil Reais) que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta.

6.4.2. O intervalo mínimo de diferença de valores entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao que cobrir a melhor oferta é de R$ 1.000,00 (um mil Reais).

6.5. Os lances serão ordenados pelo sistema e divulgados em ordem crescente, quando adotado o critério de julgamento por menor preço.

6.6. Caso o fornecedor não apresente lances, concorrerá com o valor de sua proposta.

6.7. **No modo de disputa aberto e fechado, a etapa de envio de lances terá duração de 15 minutos.**

6.7.1. Encerrado o prazo acima disposto, o sistema encaminhará o aviso de fechamento iminente dos lances e, transcorrido o período de até 10 minutos, aleatoriamente determinado pelo sistema, a recepção de lances será automaticamente encerrada.

6.7.2. Após a etapa prevista no item anterior, o sistema abrirá a oportunidade para que o autor da oferta de valor mais baixo ou de maior percentual de desconto e os autores das ofertas subsequentes com valores ou percentuais até 10% superiores ou inferiores àquela, conforme o critério adotado, possam ofertar um lance final e fechado em até 5 minutos, que será sigiloso até o encerramento deste prazo.

6.7.3. Na hipótese prevista no item anterior, o licitante poderá optar por não ofertar nenhum lance no sistema, ou optar por ofertar valor ou percentual melhor, conforme o critério de julgamento.

6.7.4. Na hipótese de haver duas ou menos propostas nas condições de que trata o item 6.7.2, serão convocados, na ordem de classificação, os autores dos três melhores lances subsequentes para oferecer um lance final e fechado nas mesmas circunstâncias.

6.7.5. Encerrado o prazo estabelecido nos itens 6.7.2 e 6.7.4, o sistema ordenará os lances conforme disposto no item 6.5.

6.8. Durante a sessão pública, os licitantes serão informados em tempo real do valor do melhor lance registrado, bem como todas as mensagens trocadas no "chat" do sistema, sendo vedada a identificação do licitante.

6.9. Na hipótese de o sistema eletrônico se desconectar no decorrer da etapa de envio de lances da sessão pública e permanecer acessível aos licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

6.10. Quando a desconexão do sistema eletrônico persistir por tempo superior a 10 minutos para a Polícia Militar de Minas Gerais, Centro de Suprimentos e Aquisições de TIC, a sessão pública será suspensa, após a finalização do envio dos lances, e reiniciada somente decorridas 24 horas após a comunicação do fato aos participantes no sítio eletrônico utilizado para divulgação.

6.11. **Do empate ficto**

6.11.1. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação junto ao CAGEF do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, regulamentada pelo Decreto Estadual nº 47.437/2018.

6.11.2. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

6.11.2.1. A melhor classificada nos termos do item anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

6.11.2.2. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

6.11.2.3. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

6.12. Em caso de empate entre duas ou mais propostas, serão utilizados os critérios de desempate previstos no art. 60 da Lei Federal nº 14.133, de 2021.

6.12.1. Na hipótese de ainda persistir o empate, haverá sorteio pelo sistema eletrônico dentre as propostas empatadas.

6.12.2. As regras previstas neste subitem não prejudicarão a aplicação do disposto no art. 44 da Lei Complementar Federal nº 123, de 14 de dezembro de 2006.

6.13. As regras de desempate não prejudicarão a aplicação do disposto no art. 44 da Lei Complementar Federal nº 123, de 14 de dezembro de 2006.

7. DO JULGAMENTO DA PROPOSTA

7.1. Encerrada a fase de lances, será verificado o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura compra, mediante a consulta aos seguintes cadastros:

CONSULTA AOS CADASTROS	FORNECEDOR PESSOA JURÍDICA - CNPJ	FORNECEDOR PESSOA FÍSICA - CPF	SÓCIO MAJORITÁRIO*- CPF ou CNPJ
CADIN – Cadastro Informativo de Inadimplência em relação à Administração Pública do Estado de Minas Gerais acessível pelo site http://consultapublica.fazenda.mg.gov.br/ConsultaPublicaCADIN/consultaSituacaoPublica.do;	SIM	SIM	NÃO
CAGEF/CAFIMP – Cadastro de Fornecedores Impedidos acessível pelo site https://www.cagef.mg.gov.br/fornecedor-web/br/gov/prodemge/seplag/fornecedor/publico/index.zul	SIM	SIM	NÃO
Consulta da situação eleitoral, acessível pelo site https://www.tse.jus.br/servicos-eleitorais/titulo-e-local-de-votacao/copy_of_consulta-por-nome	NÃO	SIM	NÃO
Certidão de Licitantes Inidôneos TCU, acessível pelo site https://contas.tcu.gov.br/ords/f?p=1660:3:111970551082228::::P3_TIPO:CPF	NÃO (Consultas já integram a certidão consolidada do TCU)	SIM	NÃO
Consulta ao Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e ao Cadastro Nacional de Empresas Punidas (CNEP) mantidos pela Controladoria-Geral da União (CGU), acessível pelo site https://certidoes.cgu.gov.br/		SIM	NÃO
Consulta ao Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade, mantido pelo Conselho Nacional de Justiça (CNJ), acessível pelo site https://www.cnj.jus.br/improbidade_adm/consultar_requerido.php?validar=form.		SIM	SIM
Consulta Consolidada de Pessoa Jurídica do TCU (Integra 4 certidões: (1) Licitantes Inidôneos, (2) CNIA - Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade, (3) CEIS - Cadastro Nacional de Empresas Inidôneas e Suspensas e (4) CNEP - Cadastro Nacional de Empresas Punidas . Acesso disponível no site https://certidoes-apf.apps.tcu.gov.br/	SIM	NÃO	NÃO
Nota: * A consulta ao cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade, mantido pelo Conselho Nacional de Justiça (CNJ) será realizada em nome do fornecedor melhor classificado e, também, de seu sócio majoritário, por força do artigo 12 da Lei n° 8.429, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.			

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

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

7.2.2. O fornecedor será convocado para manifestação previamente à sua desclassificação.

7.2.3. Constatada a existência de sanção, o fornecedor será reputado desclassificado, por falta de condição de participação.

7.3. Verificadas as condições de participação, a Administração examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos.

7.3.1. O licitante classificado em primeiro lugar deverá enviar a proposta ajustada ao último lance ofertado ou, quando não ocorrerem lances, contendo o(s) preço(s) inicialmente ofertado(s), e, se necessário, **documentos complementares, no prazo de 02 (duas) horas**, prorrogável por igual período, contado da solicitação do Pregoeiro.

7.3.1.1. A prorrogação de que trata o item acima poderá ocorrer nas seguintes situações:

7.3.1.1.1. por solicitação do licitante, mediante justificativa aceita pelo Pregoeiro;

7.3.1.1.2. de ofício, a critério do Pregoeiro, quando o substituir, quando constatado que o prazo estabelecido não é suficiente para o envio dos documentos exigidos no edital para a verificação de conformidade de que trata o item 8.1.

7.3.1.2. O fornecedor deverá realizar o upload sua proposta comercial ajustada ao seu último valor ofertado, conforme modelo constante no Anexo II - Proposta Comercial.

7.3.1.2.1. Os arquivos referentes à proposta comercial deverão ser assinados eletronicamente.

7.3.1.2.1.1. Para assinatura eletrônica, poderá ser utilizado o Portal de Assinatura Digital disponibilizado pelo Governo de Minas Gerais, de acesso gratuito, disponível em: http://www.portaldeassinaturas.mg.gov.br. Dúvidas com relação à utilização do Portal de Assinaturas Digital podem ser encaminhadas para o e-mail csa-licitacoes@pmmg.mg.gov.br, csatic.pmmg@gmail.com. A realização da assinatura digital importará na aceitação de todos os termos e condições que regem o processo eletrônico, conforme Decreto nº 47.222, de 26 de julho de 2017, e demais normas aplicáveis, admitindo como válida a assinatura eletrônica, tendo como consequência a responsabilidade pelo uso indevido das ações efetuadas e das informações prestadas, as quais serão passíveis de apuração civil, penal e administrativa.

7.3.1.2.1.2. Caso a proposta e os documentos que a acompanham sejam assinados por mandatário, deverão ser encaminhados, também a procuração e cópia da carteira de identidade do mandatário subscritor.

7.3.1.3. **O fornecedor mineiro, não optante pelo Simples Nacional, deverá informar na proposta comercial o preço resultante da dedução do ICMS e o preço com ICMS.**

7.3.1.3.1. **O disposto no subitem anterior não se aplica aos contribuintes mineiros optantes pelo Simples Nacional, devendo estes anexar à sua proposta comercial, a ficha de inscrição estadual, na qual conste a opção pelo Simples Nacional, podendo o responsável pelo procedimento, na sua falta, consultar a opção por este regime através do site: http://www8.receita.fazenda.gov.br/SimplesNacional/.**

7.4. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita da área técnica especializada no objeto.

7.5. Será desclassificada a proposta vencedora que:

7.5.1. contiver vícios insanáveis;

7.5.2. descumprir as especificações técnicas pormenorizadas contidas neste Edital, no Termo de Referência e anexos;

7.5.3. apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

7.5.4. não tiverem sua exequibilidade demonstrada, quando exigido pela Administração; e/ou

7.5.5. apresentar desconformidade com quaisquer outras exigências deste Edital e/ou do Termo de Referência e anexos, desde que insanáveis.

7.5.6. Considera-se indício de inexequibilidade a proposta que apresentar valores inferiores a 50% do valor orçado pela Administração.

7.5.6.1. A inexequibilidade, na hipótese de que trata o item anterior, somente será identificada após diligência do Pregoeiro, que comprove:

7.5.6.1.1. que o custo do licitante ultrapassa o valor da proposta;

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

7.5.7. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, deverão ser efetuadas diligências, para que o licitante comprove a exequibilidade da proposta.

7.6. Definido o resultado do julgamento, o Pregoeiro poderá negociar condições mais vantajosas com o primeiro colocado, exclusivamente por meio do Portal de Compras MG e de forma pública e transparente. O valor resultante da negociação deverá ser registrado no Portal de Compras MG.

7.6.1. Quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo ou inferior ao desconto definido para a contratação, a negociação poderá ser feita com os demais licitantes classificados, nos termos do item 8.5, respeitada a ordem de classificação, ou, em caso de propostas intermediárias empatadas, serão utilizados os critérios de desempate definidos neste edital.

7.6.2. Concluída a negociação, o resultado será registrado na ata da sessão pública, que deverá ser anexada aos autos do processo de contratação.

7.6.3. Estando o preço compatível, o licitante deverá enviar a proposta ajustada ao último valor ofertado na negociação, e, se necessário, os documentos complementares, **no prazo de 02 (duas) horas, contado da solicitação do Pregoeiro no sistema.**

7.7. Erros ou falhas no preenchimento da proposta não constituem motivo para a desclassificação. A proposta poderá ser ajustada pelo licitante, no prazo indicado pelo sistema, desde que não haja majoração do preço.

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

7.8. Se a proposta ou lance vencedor for desclassificado, o Pregoeiro examinará a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação.

7.9. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento das propostas, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo,

vinte e quatro horas de antecedência, e a ocorrência será registrada em ata.

7.10. O licitante poderá ser convocado para enviar documento digital complementar, por meio de funcionalidade de diligência disponível no sistema, **no prazo de 02 (duas) horas, sob pena de não aceitação da proposta.**

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

7.10.2. Dentre os documentos passíveis de solicitação, destacam-se os que contenham as características do bem ofertado, tais como marca, modelo, tipo, fabricante e procedência, além de outras informações pertinentes, a exemplo de catálogos, folhetos ou propostas, encaminhados por meio eletrônico, ou, se for o caso, por outro meio e prazo indicados pelo pregoeiro, sem prejuízo do seu ulterior envio pelo sistema eletrônico, sob pena de não aceitação da proposta.

7.11. **Da apresentação de amostras:**

7.11.1. Não haverá apresentação de amostras no presente certame.

8. DA HABILITAÇÃO

8.1. A verificação dos documentos será realizada por meio de consulta ao Cagef, nos documentos por ele abrangidos, assegurado aos demais participantes o direito de acesso aos dados constantes do sistema.

8.2. O licitante deverá manter atualizadas as comprovações constantes do CRC para que estejam vigentes na data da abertura da sessão pública.

8.3. Havendo a necessidade de envio de documentos complementares aos já apresentados para a habilitação, na forma estabelecida no subitem 9.1, ou de documentos não constantes do Cagef, o fornecedor melhor classificado será convocado a encaminhá-los, em formato digital, via sistema.

8.4. Nas hipóteses de exigência de apresentação de documentos de habilitação após a data de recebimentos das propostas, durante a sessão pública, os documentos deverão ser apresentados quando solicitados pelo Pregoeiro em formato digital no sistema eletrônico, por upload, **no prazo de 02 (duas) horas, prorrogável por igual período**, observadas as hipóteses elencadas no item 7.3.1.1 deste Edital.

8.4.1. A não regularização dos documentos constates do CRC no prazo do subitem anterior implicará a inabilitação do licitante, salvo se a consulta aos sítios eletrônicos oficiais emissores de certidões lograr êxito em encontrar a(s) certidão(ões) válida(s).

8.5. Após a apresentação dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para:

8.5.1. complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame;

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

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

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

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

8.7. Aos beneficiários listados no item 4.2 será concedido prazo de 05 (cinco) dias úteis, prorrogáveis por igual período, a critério da administração, para regularização da documentação fiscal e/ou trabalhista, contado a partir da divulgação da análise dos documentos de habilitação do licitante melhor classificado, conforme disposto no inciso I, do § 2º, do art. 6º do Decreto Estadual nº 47.437, de 26 de junho de 2018.

8.7.1. A não regularização da documentação no prazo deste item implicará a inabilitação do licitante vencedor, sem prejuízo das sanções previstas neste Edital, sendo facultada a convocação dos licitantes remanescentes, na ordem de classificação. Se, na ordem de classificação, seguir-se outra microempresa, empresa de pequeno porte ou sociedade cooperativa com alguma restrição na documentação fiscal e trabalhista, será concedido o mesmo prazo para regularização.

8.7.2. Se houver a necessidade de abertura do prazo para o beneficiário regularizar sua documentação fiscal e/ou trabalhista, o pregoeiro deverá suspender a sessão de pregão para o lote específico e registrar no “chat” que todos os presentes ficam, desde logo, intimados a comparecer no dia e horário informados no site www.compras.mg.gov.br para a retomada da sessão de pregão do lote em referência.

8.8. Serão disponibilizados para acesso público os documentos de habilitação dos licitantes cuja análise foi realizada pelo Pregoeiro, depois de definido o resultado do seu julgamento.

8.9. Na análise dos documentos de habilitação, o Pregoeiro poderá sanar erros ou falhas que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, e lhes atribuirá validade e eficácia para fins de habilitação, observado o disposto na Lei nº 14.184, de 31 de janeiro de 2002.

8.9.1. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas

aos saneamentos de que trata o item acima, a sessão pública somente poderá ser reiniciada mediante aviso prévio com, no mínimo, 24 horas de antecedência, e a ocorrência será registrada em ata.

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

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

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

8.12. Na hipótese de o licitante não atender às exigências para a habilitação, o órgão ou entidade examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda às especificações do objeto e as condições de habilitação.

8.13. Constatado o pleno atendimento às exigências deste instrumento convocatório, o licitante será habilitado.

9. DOS RECURSOS

9.1. Qualquer licitante poderá, durante o prazo concedido na sessão pública, não inferior a 10 minutos, de forma imediata após o término do julgamento das propostas e do ato de habilitação ou inabilitação, manifestar sua intenção de recorrer, sob pena de preclusão.

9.1.1. As razões do recurso deverão ser apresentadas em momento único, em campo próprio no sistema, no prazo de 3 dias úteis, contados a partir da notificação acerca da conclusão do juízo de admissibilidade relativo às manifestações de intenção de recorrer, realizado pelo Pregoeiro.

9.1.2. O juízo de admissibilidade referido no item 9.1.1 será realizado após a etapa de manifestação de intenção de recorrer de que trata o item 9.1, ao final da etapa de habilitação.

9.1.3. A apresentação de documentos complementares, em caso de indisponibilidade ou inviabilidade técnica ou material da via eletrônica, devidamente identificados, relativos aos recursos interpostos ou contrarrazões, se houver, será efetuada mediante envio para o e-mail pregoeiro.dts@pmmg.mg.gov.br, com cópia para csatic.pmmg@gmail.com, deve ser anexado no e-mail tela (print) comprovando a indisponibilidade técnica ou material do sistema oficial do Estado de Minas Gerais, e identificados com os dados da empresa licitante e do processo licitatório (nº. do processo e lote), observado o prazo previsto no item 9.1.

9.1.4. Os demais licitantes ficarão intimados para, se desejarem, apresentarem suas contrarrazões, no prazo de 3 dias úteis, contados da data final do prazo do recorrente, pelas mesmas formas de apresentação do recurso.

9.1.5. Será assegurada ao licitante vista dos elementos indispensáveis à defesa de seus interesses.

9.1.6. O acolhimento do recurso importará na invalidação apenas dos atos que não podem ser aproveitados.

9.1.7. Na ausência de registro de manifestação de intenção de recorrer pelos licitantes, fica a autoridade superior autorizada a adjudicar o objeto ao licitante declarado vencedor.

10. DA REVOGAÇÃO E DA ANULAÇÃO

10.1. A autoridade superior poderá revogar o procedimento licitatório pelos critérios e na forma de que trata o Decreto Estadual nº 48.723/2023 por motivo de conveniência e oportunidade, e deverá anular por ilegalidade insanável, de ofício ou por provocação de terceiros, assegurada a prévia manifestação dos interessados.

10.2. Nos casos de anulação e revogação, deverá ser assegurada a prévia manifestação dos interessados (art. 71, § 3º, Lei 14.133/21).

10.3. O motivo determinante para a revogação do processo licitatório deverá ser resultante de fato superveniente devidamente comprovado.

10.4. Ao pronunciar a nulidade, a autoridade indicará expressamente os atos com vícios insanáveis, tornando sem efeito os subsequentes que deles dependam, e dará ensejo à apuração de responsabilidade de quem lhes tenha dado causa.

10.5. Caberá recurso no prazo de 3 dias úteis contados a partir da data da anulação ou revogação da licitação, observado, no que couber, o disposto nos arts. 165 e 168 da Lei Federal nº 14.133, de 2021.

10.6. Na hipótese da ilegalidade de que trata o item 11.1 ser constatada durante a execução contratual, aplica-se o disposto no art. 147 da Lei Federal nº 14.133, de 2021.

11. DA REABERTURA DA SESSÃO PÚBLICA

11.1. Nas hipóteses de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que dele dependam.

11.1.1. Todos os licitantes remanescentes deverão ser convocados para acompanhar a sessão reaberta.

11.1.2. A convocação se dará por meio do sistema eletrônico (“chat”), quadro de avisos e também por e-mail, de acordo com a fase do procedimento licitatório.

11.1.3. A convocação feita por e-mail dar-se-á de acordo com os dados contidos no CAGEF, sendo responsabilidade do licitante manter seus dados cadastrais atualizados.

12. DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO

12.1. Encerradas as fases de julgamento e habilitação, e exauridos os recursos administrativos, o processo licitatório será encaminhado à autoridade superior, que poderá:

12.1.1. determinar o retorno dos autos para saneamento de irregularidades;

12.1.2. revogar a licitação por motivo de conveniência e oportunidade;

12.1.3. proceder à anulação da licitação, de ofício ou mediante provocação de terceiros, sempre que presente ilegalidade insanável;

12.1.4. adjudicar o objeto e homologar a licitação.

12.2. Ao homologar o procedimento, as informações serão enviadas ao PNCP automaticamente, e ficarão disponíveis para consulta no Portal de Compras.

12.2.1. A ata ficará disponível no Portal de Compras, bem como será apensada aos autos do processo de contratação.

13. DA CONTRATAÇÃO

13.1. Após a homologação, caso se conclua pela contratação, o licitante vencedor será convocado para assinar o termo de contrato ou aceitar ou retirar o instrumento equivalente, no prazo de 5 (cinco) dias úteis, a contar do recebimento da comunicação, que se dará através do sistema do Portal de Compras/MG, sob pena de decair o direito à contratação, sem prejuízo da aplicação das sanções dispostas no art. 156 da Lei Federal nº 14.133, de 2021, e outras penalidades aplicáveis.

13.1.1. O prazo de convocação poderá ser prorrogado uma vez, por igual período, mediante solicitação da parte durante seu transcurso, devidamente justificada, e desde que o motivo apresentado seja aceito pela Administração.

13.1.2. Qualquer solicitação de prorrogação de prazo para firmar o termo de contrato, aceitar ou retirar o instrumento equivalente decorrentes deste Edital, somente será analisada se apresentada antes do decurso do prazo para tal e devidamente fundamentada.

13.1.3. O adjudicatário deverá comprovar a manutenção das condições de habilitação para firmar o termo de contrato, aceitar ou retirar o instrumento equivalente, que deverão ser mantidas pelo fornecedor durante a vigência do contrato ou do instrumento equivalente.

13.1.4. Será facultado à Administração, quando o convocado não apresentar situação regular no momento de assinar o contrato, não assinar o termo de contrato ou não aceitar ou não retirar o instrumento equivalente no prazo e nas condições estabelecidas, convocar os licitantes remanescentes, na ordem de classificação, para a celebração do contrato ou retirada do instrumento equivalente, nas condições propostas pelo licitante vencedor.

13.1.5. Na hipótese de nenhum dos licitantes aceitar a contratação nos termos do item 13.1.4, a Administração, observados o valor estimado e sua eventual atualização nos termos do edital, poderá:

13.1.5.1. convocar os licitantes remanescentes para negociação, na ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço ou inferior ao desconto do adjudicatário;

13.1.5.2. adjudicar e celebrar o contrato nas condições ofertadas pelos licitantes remanescentes, atendida a ordem classificatória, quando frustrada a negociação de melhor condição.

13.1.6. A recusa injustificada do adjudicatário em assinar o contrato, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades legalmente estabelecidas e à imediata perda da garantia de proposta em favor do órgão ou da entidade promotora da licitação.

13.1.7. A regra do item 13.1.6 não se aplicará aos licitantes remanescentes convocados na forma do item 13.1.5.1.

13.1.8. O aceite da Nota de Empenho ou do instrumento equivalente, emitida ao fornecedor adjudicado, implica o reconhecimento de que:

13.1.8.1. O instrumento equivalente está substituindo o contrato, aplicando-se à relação de negócios ali estabelecida as disposições da Lei Federal nº 14.133, de 2021;

13.1.8.2. A contratada se vincula à sua proposta e às previsões contidas neste Edital e seus anexos;

13.1.9. A contratada reconhece que as hipóteses de rescisão são aquelas previstas nos artigos 137 e 138 da Lei Federal nº 14.133, de 2021, e concordam com os direitos da Administração previstos nos artigos 137 a 139 da mesma lei.

13.1.10. O prazo de vigência da contratação encontra-se previsto no Anexo I - Termo de Referência.

13.1.11. Decorrido o prazo de validade da proposta indicado no edital sem convocação para a contratação, ficarão os licitantes liberados dos compromissos assumidos.

13.1.12. O instrumento de contratação, e demais atos firmados com a Administração, serão assinados de maneira eletrônica, por intermédio do Sistema Eletrônico de Informações do Governo do Estado de Minas Gerais - SEI/MG.

13.1.12.1. Para a assinatura eletrônica, caso ainda não possua cadastro, o(s) licitante(s) interessado(s) deverá (ão) acessar o Sistema Eletrônico de Informações do Governo do Estado de Minas Gerais - SEI/MG, por meio do

link www.sei.mg.gov.br/usuarioexterno, e clicar em "Clique aqui se você ainda não está cadastrado".

13.1.12.2. Dúvidas com relação ao cadastro no SEI podem ser encaminhadas para o e-mail atendimentosei@planejamento.mg.gov.br, sei.dts@pmmg.mg.gov.br.

13.1.12.3. A realização do cadastro como Usuário Externo no SEI/MG importará na aceitação de todos os termos e condições que regem o processo eletrônico, conforme Decreto Estadual nº 47.222, de 26 de julho de 2017, e demais normas aplicáveis, admitindo como válida a assinatura eletrônica na modalidade cadastrada (login/senha), tendo como consequência a responsabilidade pelo uso indevido das ações efetuadas e das informações prestadas, as quais serão passíveis de apuração civil, penal e administrativa.

14. DA SUBCONTRATAÇÃO

14.1. A subcontratação deverá observar as disposições contidas no Anexo I - Termo de Referência.

15. DA GARANTIA FINANCEIRA DA EXECUÇÃO

15.1. Não haverá exigência de garantia financeira da execução para o presente certame.

16. DO PAGAMENTO

16.1. As condições de pagamento estão estabelecidas no Anexo I, Termo de Referência.

17. DAS SANÇÕES ADMINISTRATIVAS

17.1. As sanções administrativas incidentes estão estabelecidas no Anexo I, Termo de Referência.

18. DISPOSIÇÕES GERAIS

18.1. Este edital deverá ser lido e interpretado na íntegra, e após encaminhamento da proposta não serão aceitas alegações de desconhecimento.

18.2. O procedimento será divulgado no Portal de Compras MG e no Portal Nacional de Contratações Públicas – PNCP.

18.3. Os horários estabelecidos na divulgação deste procedimento e durante a sessão pública observarão o horário de Brasília-DF, inclusive para contagem de tempo e registro no Sistema e na documentação relativa ao procedimento.

18.4. Na contagem dos prazos estabelecidos neste edital, exclui-se o dia do início e inclui-se o do vencimento, e consideram-se os dias úteis. Só se iniciam e expiram os prazos em dia de expediente na Administração.

18.5. Havendo a necessidade de realização de ato de qualquer natureza pelos licitantes, cujo prazo não conste deste Edital, deverá ser atendido o prazo indicado pelo Pregoeiro na respectiva notificação.

18.6. É facultado ao Pregoeiro ou à Autoridade Superior, em qualquer fase do julgamento, promover diligência destinada a esclarecer ou complementar a instrução do processo e a aferição do ofertado, bem como solicitar a elaboração de pareceres técnicos destinados a fundamentar as decisões.

18.7. O objeto desta licitação deverá ser executado em conformidade com o Anexo I - Termo de Referência, correndo por conta da CONTRATADA as despesas de seguros, transporte, tributos, encargos trabalhistas e previdenciários decorrentes da execução do objeto da contratação.

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

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

18.10. O fornecedor contratado será constantemente avaliado em termos de suas entregas.

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

18.12. Fica eleito o foro da Comarca de Belo Horizonte, Estado de Minas Gerais, para dirimir eventuais conflitos de interesses decorrentes desta licitação, valendo esta cláusula como renúncia expressa a qualquer outro foro, por mais privilegiado que seja ou venha a ser.

18.13. Os interessados poderão examinar ou retirar gratuitamente o presente Edital de Licitação e seus anexos no site www.compras.mg.gov.br.

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

ANEXO DE EDITAL I - TERMO DE REFERÊNCIA
APÊNDICE I DO ANEXO DE EDITAL I - ESPECIFICAÇÃO TÉCNICA

ANEXO DE EDITAL II - MODELO DE PROPOSTA COMERCIAL PARA COMPRA DE SUBSCRIÇÃO DE SOFTWARE
ANEXO DE EDITAL III - MINUTA DE CONTRATO

Documento assinado eletronicamente por **Isabelle Almeida de Freitas**, **Assessora Jurídica**, em 17/12/2024, às 16:08, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017 .

Documento assinado eletronicamente por **Thiago Vicente de Paula e Silva**, **Major**, em 17/12/2024, às 16:44, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017 .

Documento assinado eletronicamente por **Paulo Gonçalves de Oliveira**, **Major**, em 17/12/2024, às 21:10, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017 .

A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **103463666** e o código CRC **ABD07BB6**.

Referência: Processo nº 1250.01.0011224/2024-15 SEI nº 103463666

Belo Horizonte, 18 de dezembro de 2024.

Termo Referência Pregão de Bem(Lei141333) PMMG/DTS/CSA-TIC LICITAÇÕES Nº 104183342/2024

TERMO REFERÊNCIA PREGÃO DE BEM(LEI141333)

ANEXO I - TERMO DE REFERÊNCIA DE PRESTAÇÃO DE SERVIÇO e FORNECIMENTO DE BENS (LEI 14.133)

DATA	ÓRGÃO SOLICITANTE	NÚMERO DA UNIDADE DE COMPRAS
10/12/2024	PMMG	1250071

RESPONSÁVEL PELA SOLICITAÇÃO	SUPERINTENDÊNCIA OU DIRETORIA
Diretoria de Inteligência da PMMG	Diretoria de Tecnologia e Sistemas

SUMÁRIO

1. OBJETO E CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. O presente termo de referência tem por objeto a **contratação/aquisição de Solução de Tecnologia Hiperconvergente**, nos termos da tabela abaixo e conforme condições e exigências estabelecidas neste documento.

LOTE	ITEM	CÓD. DO ITEM NO SIAD	DESCRIÇÃO SUSCINTA DO ITEM*	QUANTIDADE

01	01	001884093	Nodes de hiperconvergência (SIAD: Sistema Consolidado de Processamento de Dados...)	04
	02	001884069	Switches TOR (SIAD: Switch - Tipo: Gerenciável; Topo de Rack (TOR) LAN/SAN...)	02
	03	001836374	Solução de backup (SIAD: Servidor de rede - Tipo: Solução Hyperscale X (Backup)...)	01
	04	000050024	Serviço de Instalação (SIAD: Instalação, Configuração E Migração do Ambiente...)	01
	05	001816470	Solução de Segurança de Data Center (SIAD: Servidor de Rede - Tipo: Solução de Segurança)	01
	06	001774867	Solução de Segurança de Perímetro (SIAD: Firewall (Hardware) - Identificação: Appliance...)	02

***Em caso de divergência entre as especificações do objeto descritas no Catálogo de Materiais (CATMAS do Portal de Compras - SIAD) e as especificações técnicas constantes no Apêndice I do Anexo I - Termo de Referência/Projeto Básico, o licitante deverá obedecer a este último, pois ele contém as especificações adequadas para a demanda a ser suprida. O catálogo de materiais servirá apenas como identificação dos itens licitados e seus respectivos códigos.**

1.2. **Caracterização do Objeto**

1.2.1. O objeto desta contratação é caracterizado como comum, pois apresenta padrões de desempenho e qualidade objetivamente definidos por meio de especificações usuais de mercado.

1.3. **Lotes exclusivos para microempresas e empresas de pequeno porte**

1.3.1. 1.3.1. A participação na presente contratação é aberta a todos (sem exclusividade ou reserva de lotes para microempresas, empresas de pequeno porte e equiparados aos benefícios do Decreto nº 47.437, de 2018, e Lei Complementar nº 123, de 2006.

1.4. **Da contratação**

1.4.1. O prazo de vigência da contratação é de **05 (cinco) anos contado da publicação no Portal Nacional de Contratações Públicas - PNCP, prorrogável por até, no máximo, 10 anos**, na forma dos arts. 106 e 107 da Lei Federal nº 14.133, de 2021.

1.4.1.1. Parte da contratação é enquadrado como continuado, sendo a vigência plurianual mais vantajosa considerando Estudo Técnico Preliminar nº 98384615.

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

1.5. **Descrição da solução**

1.5.1. **A especificação do objeto está detalhada conforme Apêndice I - Especificação Técnica, deste Termo de Referência.**

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. A Polícia Militar de Minas Gerais (PMMG) possui a missão institucional de promover a segurança pública por intermédio da polícia ostensiva, com respeito aos direitos humanos e participação social em Minas Gerais seguindo a macroestratégia de polícia orientada por inteligência no combate às organizações criminosas. Está presente nos 853 (oitocentos e cinquenta e três) municípios de Minas Gerais, os quais estão sob a responsabilidade territorial das 19 (dezenove) Regiões da Polícia Militar (RPM).

2.2. Para subsidiar o alcance da missão e da visão institucionais, ambas já consolidadas no Planejamento Estratégico da PMMG, o Sistema de Inteligência da Polícia Militar (SIPOM) exerce funções essenciais, dentre elas a de difusão objetiva e oportuna de conhecimentos aos policiais militares empregados nas múltiplas atividades operacionais e o subsídio ao processo decisório com informações qualificadas e oportunas, através da aquisição de equipamentos e gestão de operações de inteligência, para fazer frente ao contexto de desenvolvimento das práticas criminosas organizadas, que podem provocar instabilidades sociais graves.

2.3. Nesse contexto, as atividades de inteligência se mostram cada vez mais preponderantes para prevenção ou repressão qualificada desses eventos. O combate às organizações criminosas se dará por dois objetivos, sendo:

• Otimizar as operações de inteligência policial militar;
• Potencializar a capacidade de primeira resposta.

2.4. Para tanto, por meio da Diretoria de Inteligência (DInt), o SIPOM tem capilaridade em todo o estado de Minas Gerais, obtendo informações das mais de 250 (duzentos e cinquenta) agências de inteligência. Além da integração interna, o estreito relacionamento com outras instituições, em especial para a repressão qualificada às organizações criminosas e as atividades ilícitas especializadas, tem se mostrado uma eficiente alternativa estratégica no enfrentamento dessa modalidade criminosa.

2.5. Neste sentido, a Inteligência Policial é o segmento fundamental para o diagnóstico e o devido assessoramento às autoridades que enfrentarão esses males. Considerada como atividade permanente e sistemática de ações especializadas para a identificação, o acompanhamento e a avaliação de ameaças reais ou potenciais na esfera da segurança pública, a Inteligência tem como objetivo prever, prevenir, neutralizar e reprimir atos criminosos, de qualquer natureza, atentatórios à ordem pública, à incolumidade das pessoas e do patrimônio.

2.6. A necessidade apresentada consiste em possibilitar o melhor suporte para a execução das atividades de Inteligência por meio da Polícia Militar, em um cenário com bancos de dados estruturados de informação (aqueles formados por tabelas planejadas) e/ou também não estruturados (informações coletadas em fonte aberta, imagens, áudios, mídias em diversos formatos), sendo necessária para tal, a substituição dos equipamentos antigos e obsoletos e aquisição de uma Central de Processamento de Dados (CPD) que suporte a hospedagem dos diversos servidores de dados e dos serviços usados pelos agentes de inteligência, isto agora em um ambiente mais seguro e eficiente para armazenar, processar e gerenciar grandes volumes de dados.

3. REQUISITOS DA CONTRATAÇÃO

3.1. Da participação de consórcios

3.1.1. Será permitida a participação de empresas reunidas em consórcio.

3.2. Da Subcontratação

3.2.1. É admitida a subcontratação parcial do objeto, limitada a 25% do serviço a ser executado.

3.3. Da Sustentabilidade

3.3.1. Não serão exigidos critérios de sustentabilidade na presente contratação, considerando o Estudo Técnico Preliminar nº 98384615.

3.4. Da indicação de marcas e modelos

3.4.1. Não serão exigidas marcas ou modelos específicos para a contratação.

3.5. Da vedação de utilização de marca ou modelo

3.5.1. Não haverá vedação de marca/modelo na presente contratação.

3.6. **Da exigência de carta de solidariedade**

3.6.1. Não será exigida a apresentação de carta de solidariedade na presente contratação.

3.7. **Da Garantia da Contratação**

3.7.1. Não será exigida garantia de execução da contratação para este objeto.

3.8. **Condições e especificações da garantia do serviço e equipamentos:**

3.8.1. Conforme APÊNDICE I DO ANEXO I – ESPECIFICAÇÃO TÉCNICA COMPRA DE BENS.

3.9. **Da vistoria**

3.9.1. Não há obrigatoriedade de realização de vistoria prévia ao local de execução dos serviços.

3.9.2. As empresas interessadas em participar poderão fazer visita ao local em, até, TRÊS DIAS ÚTEIS antes da realização do pregão para tomarem conhecimento do local e do serviço a ser executado. As visitas poderão ser agendadas pelo telefone (31) 3078-6368 ou pelo email atendimento@redesipom.mg.gov.br e ocorrerão durante o horário do expediente administrativo (de segunda à sexta-feira, de 08:30h às 12:00h ou 13:00h às 17:00h, exceto às quartas-feiras, que será de 08:30h às 13:00h). O serviço será desenvolvido na Diretoria de inteligência da PMMG, localizada à Av. Amazonas, n° 6.455, Bairro Gameleira, Belo Horizonte, MG

3.9.3. A CONTRATADA utilizará a infraestrutura de dutos de entrada no data center para interligação com seu backbone, ficando a cargo desta intervenções de pequena monta visando adaptar-se ao ambiente. Para cumprimento desta condicionante sugere-se a visita técnica aos locais para sanar eventuais dúvidas quanto à infraestrutura presente nos citados locais, conforme telefone e horários previstos no item anterior

3.9.4. No caso de o fornecedor optar por não realizar a vistoria técnica, esta pode ser substituída por declaração de que o licitante tem pleno conhecimento das condições locais e peculiaridades inerentes à natureza dos serviços, conforme Anexo III deste edital.

4. MODELO DE EXECUÇÃO DO OBJETO

4.1. Prazo e Condições da Prestação do Serviço e entrega dos equipamentos está conforme APÊNDICE I DO ANEXO I – ESPECIFICAÇÃO TÉCNICA COMPRA DE BENS.

5. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

5.1. **Condições de Recebimento**

5.1.1. **Os bens e serviços serão recebidos provisoriamente**, em até 02 (dois) dias corridos, de forma sumária, no ato da entrega, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo (a) responsável pelo acompanhamento e pela fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes na nota de empenho, no termo de referência e na proposta.

5.1.2. Os bens e serviços poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes na nota de empenho, no Termo de Referência e na proposta comercial, devendo ser substituídos no prazo estabelecido pelo Fiscal e Ordenador de Despesas, a contar da notificação do Contratado, às suas custas, sem prejuízo da aplicação das penalidades.

5.1.3. **Os bens e serviços serão recebidos definitivamente**, após a verificação da qualidade e quantidade do material, bem como o atendimento das exigências contratuais e consequente aceitação, que deverá acontecer, mediante termo detalhado, em até 20 (vinte) dias corridos, a partir do recebimento provisório. O prazo poderá ser prorrogado desde que justificada mediante análise da complexidade técnica, ou alto volume de aquisições, ou por

ocorrência de evento superveniente, devidamente justificado pelo fiscal do contrato e aprovado pelo Ordenador de Despesas.

5.1.4. 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 Federal nº 14.133, de 2021, a Administração notificará o Contratado para emissão de Nota Fiscal no que diz respeito à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

5.1.5. 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.

5.1.6. O recebimento/aprovação do(s) produto(s) pelo Contratante não exclui a responsabilidade civil do Contratado por vícios de quantidade ou qualidade do(s) produto(s) ou disparidades com as especificações estabelecidas, verificadas posteriormente, garantindo-se à Administração as faculdades previstas no art. 18 da Lei Federal n.º 8.078, de 1990.

5.2. **Da Liquidação**

5.2.1. A Liquidação será efetuada no prazo de até 08 (oito) dias corridos contados da data da entrega definitiva do serviço e respectivo aceite do Contratante.

5.2.2. 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:

5.2.2.1. O vencimento;

5.2.2.2. A data de emissão;

5.2.2.3. Os dados do contrato e do órgão contratante;

5.2.2.4. O período respectivo de execução do objeto;

5.2.2.5. O valor a pagar; e

5.2.2.6. Eventual destaque do valor de retenções tributárias cabíveis.

5.2.3. 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.

5.2.4. A nota fiscal ou o instrumento de cobrança equivalente deverá ser acompanhado da comprovação da regularidade fiscal disposta no art. 68 da Lei Federal nº 14.133, de 2021.

5.3. **Do pagamento**

5.3.1. O pagamento será efetuado através do Sistema Integrado de Administração Financeira - SIAFI/MG, por meio de ordem bancária emitida por processamento eletrônico, a crédito do beneficiário em um dos bancos que o Contratado indicar, no prazo de até 30 (trinta) dias corridos, contados a partir da data final da liquidação a que se referir, com base nos documentos fiscais devidamente conferidos e aprovados pelo Contratante.

5.3.1.1. A Administração deve observar a ordem cronológica nos pagamentos, conforme disposto no art. 141 da Lei Federal nº 14.133, de 2021.

5.3.2. No caso de atraso pelo Contratante, por culpa exclusiva da Administração, os valores devidos ao Contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, de acordo com a variação do IPCA.

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

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

5.3.5. A CONTRATADA deve garantir a manutenção dos requisitos de habilitação previstos no Edital.

5.3.5.1. Eventuais situações de irregularidades fiscal ou trabalhista da CONTRATADA não impedem o pagamento, se o objeto tiver sido executado e atestado. Tal hipótese ensejará, entretanto, a adoção das providências tendentes ao sancionamento do contratado e rescisão contratual.

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

6. PROCEDIMENTO DE TRANSIÇÃO E FINALIZAÇÃO DO CONTRATO

6.1. Será obrigação da empresa contratada todo o suporte necessário para transição e finalização do contrato, conforme necessidades apontadas pelo fiscal do contrato no momento de encerramento.

7. MODELO DE GESTÃO DA CONTRATAÇÃO

7.1. Regras Gerais

7.1.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as disposições da Lei Federal nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial, conforme art. 115 da Lei Federal nº 14.133, de 2021, e artigos 15 e 16 do Decreto 48.587, de 2023.

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

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

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

7.1.5. A execução do contrato deverá ser acompanhada e fiscalizada por 1 (um) ou mais gestores e fiscais do contrato, representantes da Administração especialmente designados conforme requisitos estabelecidos no art. 7º da Lei Federal nº 14.133, de 2021, ou pelos respectivos substitutos, conforme art. 117 da Lei Federal nº 14.133, de 2021, e art. 14 do Decreto nº 48.587, de 2023.

7.1.6. Constatada a ocorrência de descumprimento total ou parcial do contrato, deverão ser observadas as disposições dos art. 155 a 163 da Lei Federal nº 14.133, de 2021, a fim de apurar a responsabilidade do Contratado e eventualmente aplicar sanções.

7.2. Da Fiscalização do Contrato

7.2.1. O fiscal do contrato prestará apoio técnico e operacional ao gestor do contrato com informações pertinentes as suas competências, nos termos do inciso I do art. 16 do Decreto nº 48.587, de 2023.

7.2.2. O fiscal do contrato anotará em registro próprio todas as ocorrências relacionadas à execução do contrato, determinando o que for necessário para a regularização das faltas ou dos defeitos observados, de acordo com o § 1º, art. 117 da Lei Federal nº 14.133, de 2021, e inciso II do art. 16 do Decreto nº 48.587, de 2023.

7.2.3. O fiscal do contrato emitirá notificações para a correção de rotinas ou de qualquer inexatidão ou irregularidade constatada, com a definição de prazo para a correção, nos termos do inciso III do art. 16 do Decreto nº 48.587, de 2023.

7.2.4. O fiscal do contrato informará a seus superiores e ao gestor do contrato, em tempo hábil para a adoção das medidas convenientes, a situação que demandar decisão ou providência que ultrapasse sua competência, conforme § 2º, art. 117 da Lei Federal nº 14.133, de 2021, e inciso IV do art. 16 do Decreto nº 48.587, de 2023.

7.2.5. O fiscal do contrato comunicará imediatamente ao gestor do contrato quaisquer ocorrências que possam inviabilizar a execução do contrato nas datas estabelecidas, nos termos do inciso V, do art. 16 do Decreto nº 48.587, de 2023.

7.2.6. O fiscal do contrato fiscalizará a execução do contrato para que sejam cumpridas as condições estabelecidas, de modo a assegurar os melhores resultados para a Administração, com a conferência das notas fiscais e das documentações exigidas para o pagamento e, após o ateste, que certifica o recebimento provisório, encaminhar ao gestor de contrato, nos termos do inciso VI, do art. 16 do Decreto nº 48.587, de 2023.

7.2.7. O fiscal do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual, nos termos do inciso VII, do art. 16 do Decreto nº 48.587, de 2023.

7.2.8. O fiscal do contrato realizará o recebimento provisório do objeto do contrato, mediante termo detalhado que comprove o cumprimento das exigências contratuais, nos termos do inciso VIII, do art. 16 do Decreto nº 48.587, de 2023.

7.2.9. A fiscalização de que trata esta cláusula não exclui, nem reduz a responsabilidade do Contratado por quaisquer irregularidades, inexecuções ou desconformidades havidas na execução do objeto, aí incluídas imperfeições de natureza técnica ou aquelas provenientes de vício redibitório, como tal definido pela lei civil.

7.3. **Da Gestão do Contrato**

7.3.1. O gestor do contrato orientará os fiscais de contrato no desempenho de suas atribuições, nos termos do inciso I, do art. 15 do Decreto nº 48.587, de 2023.

7.3.2. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato ou terceiros contratados, das ocorrências relacionadas à execução do contrato e as medidas adotadas, e informará à autoridade superior àquelas que ultrapassarem a sua competência, nos termos do inciso II, do art. 15 do Decreto nº 48.587, de 2023.

7.3.3. O gestor do contrato acompanhará a manutenção das condições de habilitação do contratado, para fins de empenho de despesa e de pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais, nos termos do inciso III, do art. 15 do Decreto nº 48.587, de 2023.

7.3.4. O gestor do contrato coordenará a autuação da rotina de acompanhamento e de fiscalização do contrato, cujo histórico de gerenciamento deverá conter todos os registros formais da execução, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, nos termos do inciso IV, do art. 15 do Decreto nº 48.587, de 2023.

7.3.5. O gestor do contrato coordenará os atos preparatórios relativos à instrução processual e ao envio da documentação pertinente ao setor de contratos para formalização da celebração de aditivos, prorrogações, reajustes, repactuações ou rescisões contratuais, nos termos do inciso V, do art. 15 do Decreto nº 48.587, de 2023.

7.3.6. O gestor do contrato realizará o recebimento definitivo do objeto do contrato, mediante termo detalhado que comprove o atendimento das exigências contratuais, nos termos do inciso VI, do art. 15 do Decreto nº 48.587, de 2023.

7.3.7. O gestor do contrato elaborará o relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem

adotadas para o aprimoramento das atividades da Administração, de que trata a alínea "d" do inciso VI do § 3º do art. 174 da Lei Federal nº 14.133, de 2021, nos termos do inciso VII, do art. 15 do Decreto nº 48.587, de 2023.

7.3.8. O gestor do contrato tomará as providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei Federal nº 14.133, de 2021, ou pelo agente ou pelo setor competente para tal, conforme o caso, nos termos do inciso VIII, do art. 15 do Decreto nº 48.587, de 2023.

7.3.9. Poderá a Administração designar o mesmo servidor para as funções de fiscal e gestor do contrato, conforme § 3, Art. 8º do Decreto Estadual nº 46.944, de 29/01/2016.

8. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

8.1. O fornecedor será selecionado por meio da realização de procedimento na modalidade pregão, conforme art. 28 da Lei Federal nº 14.133, de 2021, sob a forma eletrônica, com adoção do critério de julgamento pelo menor preço, conforme art. 33, da referida Lei Federal, tendo em vista a justificativa apresentada no Estudo Técnico Preliminar nº 98384615.

8.2. **Dos critérios de aceitabilidade da proposta**

8.2.1. A proposta terá validade de 90 (noventa) dias corridos contados da data de aceitação.

8.3. **Da prova de Conceito**

8.3.1. Não será exigida a apresentação de prova de conceito nesta contratação.

9. HABILITAÇÃO

9.1. **Habilitação Jurídica**

9.1.1. Documento de identificação, com foto, do responsável pela(s) assinatura(s) da(s) Proposta(s) Comercial(is).

9.1.2. Registro empresarial na Junta Comercial, no caso de empresário individual.

9.1.3. Ato constitutivo, estatuto ou contrato social e suas alterações posteriores ou instrumento consolidado, devidamente registrado na Junta Comercial, em se tratando de sociedades empresárias, cooperativas ou empresas individuais de responsabilidade limitada e, no caso de sociedade de ações, acompanhado de documentos de eleição ou designação de seus administradores.

9.1.4. Ato constitutivo devidamente registrado no Registro Civil de Pessoas Jurídicas em se tratando de sociedade não empresária, acompanhado de prova da diretoria em exercício.

9.1.5. Decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no País.

9.1.6. Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

9.2. **Habilitação Fiscal, Social e Trabalhista**

9.2.1. Inscrição no Cadastro de Pessoas Físicas (CPF) ou no Cadastro Nacional da Pessoa Jurídica (CNPJ).

9.2.2. Inscrição no cadastro de contribuintes estadual e/ou municipal, se houver, relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual.

9.2.3. Regularidade perante a Fazenda federal, estadual e/ou municipal do domicílio ou sede do fornecedor, ou outra equivalente, na forma da lei.

9.2.3.1. A prova de regularidade fiscal e seguridade social perante a Fazenda Nacional será efetuada mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil – RFB e pela Procuradoria-Geral da Fazenda Nacional – PGFN, referente a todos os tributos federais e à Dívida Ativa da União – DAU por elas administrados, bem como das contribuições previdenciárias e de terceiros.

9.2.3.2. Caso o fornecedor seja considerado isento dos tributos estaduais e/ou municipais objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

9.2.4. Certificado de Regularidade relativa à seguridade social e perante o Fundo de Garantia por Tempo de Serviço –FGTS.

9.2.5. Prova de inexistência de débitos inadimplidos perantea Justiça do Trabalho, mediante a apresentação de certidão negativa, ou positiva com efeito de negativa, nos termos da Lei Federal nº 12.440, de 7 de julho de 2011, 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.

9.2.6. Comprovação da regularidade fiscal e/ou trabalhista deverá ser efetuada mediante a apresentação das competentes certidões negativas de débitos, ou positivas com efeitos de negativas.

9.3. **Qualificação Econômico-Financeira**

9.3.1. Certidão negativa de feitos sobre falência expedida pelo distribuidor da sede do fornecedor, emitida nos últimos 06 (seis) meses.

9.3.2. **Balanço patrimonial,** demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais.

9.3.2.1. Serão aceitos como na forma da Lei o Balanço Patrimonial e demonstrações contábeis assim apresentados:

9.3.2.1.1. Sociedades regidas pela Lei Federal nº 6.404/76 (Sociedade Anônima):

9.3.2.1.1.1. Publicadas em Diário Oficial; ou

9.3.2.1.1.2. Publicados em jornal; ou

9.3.2.1.1.3. Por cópia registrada ou autenticada na Junta Comercial da sede ou domicílio do licitante;

9.3.2.1.2. Sociedades Limitadas (LTDA):

9.3.2.1.2.1. Por cópia do Livro Diário, devidamente autenticado na Junta Comercial da sede ou domicílio do licitante ou em outro órgão equivalente, inclusive com os Termos de Abertura e de Encerramento; ou

9.3.2.1.2.2. Por cópia do Balanço e das Demonstrações Contábeis devidamente registrados ou autenticados na Junta Comercial da sede ou do domicílio do licitante.

9.3.2.1.3. Sociedades sujeitas ao regime estabelecido na Lei Complementar Federal nº 123/06 (Lei das Microempresas e das Empresas de Pequeno Porte) – "SIMPLES NACIONAL":

9.3.2.1.3.1. Por cópia do Balanço e das Demonstrações Contábeis devidamente registrados ou autenticados na Junta Comercial da sede ou do domicílio do licitante;

9.3.2.2. Os documentos exigidos no subitem 9.3.2.2, quando forem próprios, deverão ser assinados pelo representante legal do licitante e pelo seu contador ou, quando publicados em Órgão de Imprensa Oficial, deverão permitir a identificação do veículo e

da data de sua publicação e conter o nome do contador e o número de seu registro no Conselho Regional de Contabilidade.

9.3.2.3. As pessoas jurídicas obrigadas a adotar a Escrituração Contábil Digital– ECD, bem como as sociedades empresárias que facultativamente aderiram ao sistema, nostermos da Instrução Normativa da Receita Federal doBrasil nº 1.774, de 2017, poderão apresentar a ECD para os fins previstos no subitem 9.3.2.2.

9.3.2.4. Índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), comprovados mediante a apresentação pelo fornecedor de balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais e obtidos pela aplicação das seguintes fórmulas:

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

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

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

9.3.2.5. Caso a empresa fornecedora apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação patrimônio líquido mínimo de 1 (um)% do valor total estimado da compra.

9.3.2.5.1. Para os casos de consórcios, exceto os consórcios compostos, em sua totalidade, de microempresas e pequenas empresas, caso o licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação patrimônio líquido mínimo de 10 (dez)% do valor total estimado da contratação.

9.3.2.6. As empresas criadas no exercício financeiro da contratação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura, conforme disposto no art. 65, §1º da Lei Federal nº 14.133, de 2021.

9.3.2.7. O balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos.

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

9.3.2.9. Caso o fornecedor seja cooperativa, tais documentos deverão ser acompanhados da última auditoria contábil-financeira, conforme dispõe o artigo 112 da Lei Federal nº 5.764, de 1971, ou de uma declaração, sob as penas da lei, de que tal

auditoria não foi exigida pelo órgão fiscalizador.

9.4. **Da Qualificação Técnico-Operacional e Técnico-Profissional**

9.4.1. Não será exigida a apresentação de documentos relativos à qualificação técnico-profissional.

9.4.2. A qualificação técnico-Operacional está detalhada conforme Apêndice I do Anexo I - Especificação Técnica.

9.4.2.1. Os atestados de qualificação técnico-Operacional deverão conter:

9.4.2.1.1. Nome empresarial e dados de identificação da instituição emitente (CNPJ, endereço, contato);

9.4.2.1.2. Local e data de emissão;

9.4.2.1.3. Nome, cargo, contato e a assinatura do responsável pela veracidade das informações;

9.4.2.1.4. Período da execução da atividade e quantitativo do objeto fornecido.

9.4.2.2. Os atestados de capacidade técnica (qualificação técnico-Operacional) poderão ser apresentados em nome da matriz ou da filial do fornecedor.

9.4.2.3. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual do Contratante e local em que foi executado o objeto contratado, dentre outros documentos.

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

9.4.2.5. Em caso de apresentação por de atestado de desempenho anterior emitido em favor de consórcio do qual o fornecedor tenha feito parte, se o atestado ou o contrato de constituição do consórcio não identificar a atividade desempenhada por cada consorciado individualmente, serão adotados os seguintes critérios na avaliação de sua qualificação técnica:

9.4.2.5.1. Caso o atestado tenha sido emitido em favor de consórcio homogêneo, cujas empresas possuem objeto social similar, as experiências atestadas deverão ser reconhecidas para cada empresa consorciada na proporção quantitativa de sua participação no consórcio.

9.4.2.5.2. Caso o atestado tenha sido emitido em favor de consórcio heterogêneo, cujas empresas possuem objeto social diverso, as experiências atestadas deverão ser reconhecidas para cada consorciado de acordo com os respectivos campos de atuação.

9.4.5.3. Na hipótese do item 9.4.5, para fins de comprovação do percentual de participação do consorciado, caso este não conste expressamente do atestado ou da certidão, deverá ser juntada ao atestado ou à certidão cópia do instrumento de constituição do consórcio.

9.5. **Habilitação de Consórcios:**

9.5.1. No caso da participação de empresas reunidas em consórcio, deverá acompanhar os documentos de habilitação, a comprovação de compromisso público ou particular do consórcio, subscrito pelas empresas consorciadas, com apresentação da proporção de participação de cada uma das consorciadas e indicação da empresa líder, que deverá

representar as consorciadas perante o Estado de Minas Gerais, observadas as normas do art. 15 da Lei Federal nº 14.133, de 2021.

9.5.2. Deverão ser apresentados os documentos previstos no item referente à Habilitação, por parte de cada consorciado, admitindo-se, para efeito de qualificação técnica, o somatório dos quantitativos de cada consorciado, e, para efeito de qualificação econômico-financeira, o somatório dos valores de cada consorciado, na proporção de sua respectiva participação.

9.5.3. As empresas consorciadas serão solidariamente responsáveis pelas obrigações do consórcio na fase de licitação e durante a execução do contrato.

9.5.4. Antes da celebração do contrato, deverá ser promovida a constituição e o registro do consórcio, nos termos do compromisso referido no item 9.5.1.

9.5.5. Apenas os consórcios compostos exclusivamente por beneficiários indicados no item 4.3 poderão usufruir dos benefícios legais da Lei Complementar Federal nº 123, de 14 de dezembro de 2006, desde que a soma do faturamento das empresas consorciadas não ultrapasse o limite previsto no inciso II, artigo 3º, da Lei Complementar Federal nº 123, de 14 de dezembro de 2006.

9.5.6. Não é permitido que uma empresa, consorciada simultaneamente em mais de um consórcio ou de forma isolada, participe do mesmo procedimento de contratação.

9.5.7. A substituição de consorciado deverá ser expressamente autorizada pelo órgão ou entidade contratante e condicionada à comprovação de que a nova empresa do consórcio possui, no mínimo, os mesmos quantitativos para efeito de habilitação técnica e os mesmos valores para efeito de qualificação econômico-financeira apresentados pela empresa substituída para fins de habilitação do consórcio no processo licitatório que originou o contrato.

9.6. **Habilitação de Cooperativas**

9.6.1. Caso admitida a participação de cooperativas, os profissionais organizados sob a forma de cooperativa poderão participar de licitação quando:

9.6.1.1. A constituição e o funcionamento da cooperativa observarem as regras estabelecidas na legislação aplicável, em especial aLei nº 5.764, de 16 de dezembro de 1971, aLei nº 12.690, de 19 de julho de 2012, e aLei Complementar nº 130, de 17 de abril de 2009;

9.6.1.2. A cooperativa apresentar demonstrativo de atuação em regime cooperado, com repartição de receitas e despesas entre os cooperados;

9.6.1.3. Qualquer cooperado, com igual qualificação, for capaz de executar o objeto contratado, vedado à Administração indicar nominalmente pessoas.

9.6.2. Será exigida a seguinte documentação complementar:

9.6.2.1. A relação dos cooperados que atendem aos requisitos técnicos exigidos para a contratação e que executarão o contrato, com as respectivas atas de inscrição e a comprovação de que estão domiciliados na localidade da sede da cooperativa, respeitado o disposto nos arts. 4º, inciso XI, 21, inciso I e 42, §§2º a 6º da Lei n. 5.764, de 1971.

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

9.6.2.3. A comprovação do capital social proporcional ao número de cooperados necessários à execução contratual.

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

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

9.6.2.6. A última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei n. 5.764, de 1971, ou uma declaração, sob as penas da lei, de que tal

auditoria não foi exigida pelo órgão fiscalizador.

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

10. OBRIGAÇÕES ESPECÍFICAS DAS PARTES

10.1. Do Contratante

10.1.1. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o presente termo de referência, contrato e eventuais anexos.

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

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

10.1.4. Acompanhar e fiscalizar a execução do contrato, atestar nas notas fiscais/faturas da efetiva prestação de serviço, objeto do Termo de Referência.

10.1.5. Rejeitar, no todo ou em parte os serviços prestados, quando em desacordo com as especificações constantes na nota de empenho, no Termo de Referência e/ou na proposta comercial do Contratado, impondo-se a recusa se o objeto for defeituoso, tiver prazo de validade vencido, ou outras situações que inviabilizem o recebimento, hipótese em que se promoverá anotação da ocorrência em registro próprio.

10.1.6. Solicitar o reparo, a correção, a remoção ou a substituição da parcela do objeto em que se verificarem vícios, defeitos ou incorreções.

10.1.7. Efetuar o pagamento ao Contratado do valor correspondente à parcela do serviço prestado, no prazo, forma e condições estabelecidos no presente instrumento.

10.1.8. Prestar as informações e os esclarecimentos que venham a ser solicitados pelo Contratado.

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

10.1.9.1. A Administração terá o prazo de até 15 (quinze) dias corridos a contar da data do protocolo do requerimento, tratado no item 10.1.9, para decidir e admitir a prorrogação motivada por igual período, conforme art. 123, Lei Federal nº 14.133, de 2021.

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

10.1.11. Aplicar ao Contratado as sanções regulamentares.

10.1.12. Exigir o cumprimento dos recolhimentos tributários, trabalhistas e previdenciários por meio dos documentos pertinentes.

10.1.13. Disponibilizar local adequado para a realização do serviço.

10.1.14. 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.

10.2. **Do Contratado**

10.2.1. O Contratado deve cumprir todas as obrigações constantes deste instrumento e seus anexos, nas quantidades, prazos e condições pactuadas, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto.

10.2.2. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com o Código de Defesa do Consumidor, Lei Federal nº 8.078, de 1990.

10.2.3. 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.

10.2.4. Atender às determinações regulares emitidas pelo fiscal ou gestor do contrato ou autoridade superior, conforme Inciso II, art. 137 da Lei Federal nº 14.133, de 2021, e inciso III, art. 16 do Decreto nº 48.587, de 2023, e prestar todo esclarecimento ou informação por eles solicitados.

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

10.2.6. O contratado será responsável pelos danos causados diretamente à Administração ou a terceiros em razão da execução do contrato, e não excluirá nem reduzirá essa responsabilidade a fiscalização ou o acompanhamento pelo contratante.

10.2.7. Não contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do contratante ou do fiscal ou gestor do contrato, nos termos do art. 48, parágrafo único, da Lei Federal nº 14.133, de 2021.

10.2.8. Emitir faturas no valor pactuado, apresentando-as ao Contratante para ateste e pagamento.

10.2.9. Responsabilizar-se pela garantia dos materiais empregados nos serviços prestados, dentro dos padrões adequados de qualidade, segurança, durabilidade e desempenho, conforme previsto na legislação em vigor e na forma exigida neste termo de referência.

10.2.10. 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.

10.2.11. 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.

10.2.12. 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.

10.2.13. 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.

10.2.14. 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 em outras normas específicas, conforme art. 116 da Lei Federal nº 14.133, de 2021.

10.2.14.1. Comprovar a reserva de cargos a que se refere a cláusula acima, quando solicitado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas, conforme parágrafo único, art. 116 da Lei Federal nº 14.133, de 2021.

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

10.2.16. 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 inciso II, alínea d, art. 124 da Lei Federal nº 14.133, de 2021.

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

10.2.18. Alocar os empregados necessários, com habilitação e conhecimento adequados, ao perfeito cumprimento das cláusulas do 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.

10.2.19. Orientar e treinar seus empregados sobre os deveres previstos na Lei Federal nº 13.709, de 2018, adotando medidas eficazes para proteção de dados pessoais a que tenha acesso por força da execução deste contrato.

10.2.20. 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.

10.2.21. 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.

10.2.22. 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.

10.3. **Do Preposto**

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

11. INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

11.1. Comete infração administrativa, nos termos da Lei Federal nº 14.133, de 2021, o contratado que:

11.1.1. Der causa à inexecução parcial da contratação;

11.1.2. Der causa à inexecução parcial da contratação que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

11.1.3. Der causa à inexecução total da contratação;

11.1.4. Deixar de entregar a documentação exigida para o certame;

11.1.5. Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

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

11.1.7. Ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

11.1.8. Apresentar documentação falsa ou prestar declaração falsa durante a contratação e execução do contrato;

11.1.9. Fraudar a licitação ou praticar ato fraudulento na execução da contratação;

11.1.10. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

11.1.11. Praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

11.1.12. Praticar ato lesivo previsto no art. 5º da Lei Federal nº 12.846, de 2013.

11.2. Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:

11.2.1. **Advertência** - quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave, conforme disposto no §2º, art. 156 da Lei Federal nº 14.133, de 2021;

11.2.2. **Impedimento de licitar e contratar** - quando praticadas as condutas descritas nos subitens 11.1.2 a 11.1.7, sempre que não se justificar a imposição de penalidade mais grave, conforme disposto no § 4º, art. 156, da Lei Federal nº 14.133, de 2021;

11.2.3. **Declaração de inidoneidade para licitar e contratar** - quando praticadas as condutas descritas nos subitens 11.1.8 a 11.1.12, bem como nos subitens 11.1.2 a 11.1.7, que justifiquem a imposição de penalidade mais grave, conforme disposto no §5º, art. 156, da Lei Federal nº 14.133, de 2021);

11.2.4. **Multa:**

11.2.4.1. 0,5% (cinco décimos de por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida (fornecimento não realizado), até o limite de 30 (trinta) dias, observando o item 11.2.4.4.

11.2.4.2. 20% (vinte por cento) sobre o valor da parcela inadimplida, após ultrapassado o prazo de 30 dias de atraso, ou no caso de não entrega do objeto, ou entrega com vícios ou defeitos ocultos que o torne impróprio ao uso a que é destinado, ou diminua-lhe o valor ou, ainda fora das especificações contratadas; observando o item 11.2.4.4.

11.2.4.3. 2% (dois por cento) sobre o valor total do contrato, em caso de descumprimento das demais obrigações contratuais ou norma da legislação pertinente.

11.2.4.4. Conforme Art. 156, §3º, da Lei Federal nº 14.133, de 2021, independente dos valores obtido nos itens anteriores, a multa mínima será de 0,5% (cinco décimos de por cento) e a máximo será de 30 % (trinta por cento), ambos sobre o valor total do contrato.

11.3. As sanções previstas nos subitens 11.2.1, 11.2.2 e 11.2.3 poderão ser aplicadas cumulativamente com a multa, conforme disposto no §7º, art. 156, da Lei Federal nº 14.133, de 2021.

11.4. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente, conforme §8º, art. 156, da Lei Federal nº 14.133, de 2021.

11.5. A aplicação das sanções previstas neste documento não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante, conforme disposto no §9º, art. 156, da Lei Federal nº 14.133, de 2021.

11.6. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, conforme disposto no art. 157, da Lei Federal nº 14.133, de 2021.

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

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

11.9. Em observância ao disposto no §1º, art. 156, da Lei Federal nº 14.133, de 2021, na aplicação das sanções serão considerados:

11.9.1. A natureza e a gravidade da infração cometida;

11.9.2. As peculiaridades do caso concreto;

11.9.3. As circunstâncias agravantes ou atenuantes;

11.9.4. Os danos que dela provierem para o Contratante;

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

11.10. Os atos previstos como infrações administrativas na Lei Federal nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei Federal nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos nesta última Lei citada, conforme art. 159 da referida Lei de Licitações.

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

11.12. O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e no Cadastro Nacional de Empresas Punidas (CNEP), instituídos no âmbito do Poder Executivo Federal, conforme art. 161, da Lei Federal nº 14.133, de 2021.

11.13. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei Federal nº 14.133, de 2021.

11.14. Os débitos do contratado para com a Administração contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o contratado possua com o mesmo órgão ora contratante.

12. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

12.1. O custo estimado da contratação possui caráter sigiloso, tendo em vista a justificativa apresentada no Estudo Técnico Preliminar SEI nº 98384615.

13. ADEQUAÇÃO ORÇAMENTÁRIA

13.1. As despesas decorrentes da presente contratação correrão por conta da dotação orçamentária do orçamento em vigor, aprovado pela Lei Estadual nº 24.678/2024 - Lei Orçamentária Anual (LOA).

13.1.1. A contratação será atendida pela seguinte dotação:
1251 6 181 137 4365 1 3 3 90 39 21 0 9 1,
1251 6 181 137 4365 1 4 4 90 52 7 0 9 1.

13.1.2. Convênio nº 9413748.

13.2. A dotação relativa ao exercício financeiro subsequente será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

Documento assinado eletronicamente por **Renato Silveira Fernandes**, **2º Tenente**, em 18/12/2024, às 21:09, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

Documento assinado eletronicamente por **Thiago Vicente de Paula e Silva**, **Major**, em 18/12/2024, às 21:47, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **104183342** e o código CRC **72A31FD3**.

Referência: Processo nº 1250.01.0011224/2024-15 SEI nº 104183342

Especificação de Material/Serviço PMMG/DINT nº. 8/2024

Belo Horizonte, 18 de dezembro de 2024.

ESPECIFICAÇÃO TÉCNICA PARA COMPRA DE BENS (PREGÃO)

APÊNDICE I DO ANEXO I – ESPECIFICAÇÃO TÉCNICA COMPRA DE BENS

DATA	ÓRGÃO SOLICITANTE	NÚMERO DA UNIDADE DE COMPRA
04/11/2024	Diretoria de Inteligência	1250071

RESPONSÁVEL PELA SOLICITAÇÃO	DIRETORIA PMMG
Diretoria de Inteligência	Diretoria de Tecnologia e Sistemas

Sumário

1. OBJETO E CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. A presente ESPECIFICAÇÃO TÉCNICA tem por objeto a aquisição de Solução de Tecnologia Hiperconvergente, sob a forma de entrega integral realizada em 1 LOTE, sendo obrigatório o fornecimento pelo mesmo licitante, em vista da padronização integral da solução nos termos da tabela abaixo e conforme condições e exigências estabelecidas neste documento.

LOTE	ITEM	CÓD. DO ITEM NO SIAD	DESCRIÇÃO SUSCINTA DO ITEM	UNIDADE DE AQUISIÇÃO	QUANTIDADE
	01	001884093	Nodes de hiperconvergência	CSA-TIC	04
	02	001884069	Switches TOR	CSA-TIC	02
	03	001836374	Solução de backup	CSA-TIC	01
	04	000050024	Serviço de Instalação	CSA-TIC	01
	05	001816470	Solução de Segurança de Data Center	CSA-TIC	01
	06	001774867	Solução de Segurança de Perímetro	CSA-TIC	02

*** Em caso de divergência entre as especificações do objeto descritas no Catálogo de Materiais (CATMAS do Portal de Compras) e as especificações técnicas constantes no Apêndice I do Anexo I - ESPECIFICAÇÃO TÉCNICA , o licitante deverá obedecer a este último, pois ele contém as especificações adequadas para a demanda a ser suprida. O catálogo de materiais servirá apenas como identificação dos itens licitados e seus respectivos códigos.**

*** O preenchimento dos campos do sistema bem como o arquivo referente a Proposta Comercial anexada deverá se referir, individualmente, para cada lote.**

1.2. **Caracterização do Objeto:**

1.2.1. O objeto desta contratação é caracterizado como comum, pois apresenta padrões de desempenho e qualidade objetivamente definidos por meio de especificações usuais de mercado.

1.2.2. O objeto desta contratação não se enquadra como sendo bem de luxo, conforme Decreto nº 48.586, de 2023.

1.3. **Lotes exclusivos para microempresas e empresas de pequeno porte:**

1.3.1 A participação na presente contratação é aberta a todos (sem exclusividade ou reserva de lotes para microempresas, empresas de pequeno porte e equiparados aos benefícios do Decreto no 47.437, de 2018, e Lei Complementar no 123, de 2006).

1.4 Descrição da Solução:

1.4.1. **Appliance Híbrido de Hiperconvergência**

1.4.1.1. O appliance de hiperconvergência deve vir novo de fábrica.

1.4.1.2. Serão aceitos somente appliances, desde que garantida a compatibilidade com a ferramenta de gestão e atualização dos firmwares e softwares relacionados à infraestrutura hiperconvergente (virtualização e armazenamento definidos por software) de maneira centralizada, automatizada e orquestrada. Todos os componentes de hardware deverão ser totalmente compatíveis com os softwares especificados neste termo de referência.

1.4.1.3. A marca e o modelo dos appliances ofertados deverão ter todos os componentes de hardware compatíveis com os softwares especificados neste termo de referência;

1.4.1.4. Os equipamentos deverão ser integrados logicamente previamente, com seus componentes interligados sem ponto único de falha e de acordo com as melhores práticas do fabricante, após a energização e conexão física e lógica do sistema;

1.4.1.5. A solução inicial deve fornecer, no mínimo, 4 (quatro) nós, ou mais, cada um com capacidade de computação conforme especificações a seguir:

1.4.1.5.1. O equipamento deve possuir chassi que permita instalação rack padrão 19”, com altura de 2U com no mínimo 10 (dez) baias de discos hotswap de 3,5 polegadas frontal.

1.4.1.5.2. Cada chassi deve possuir no mínimo 1 (um) nó, sendo que este nó corresponde a uma unidade

física de processamento e armazenando da solução hiperconvergente dos processadores (CPU), memória (RAM), discos locais (SSD e HDD's), interfaces de comunicação (NICs) e software hiperconvergente.

1.4.1.4.1.5.3. Devem ser fornecidos todos os acessórios necessários para sua instalação, incluindo, mas não se limitando a trilhos para montagem em rack, cabos de alimentação e de todas as licenças de softwares necessárias para o funcionamento da solução conforme requisitos mínimos.

1.4.1.5.4. Display ou LEDs frontal embutido no gabinete para monitoramento das condições de funcionamento dos principais componentes do servidor através da exibição de alertas de falha.

1.4.1.5.5. Deve possuir, no mínimo:

1.4.1.5.5.1. Uma porta USB 3.1 e uma porta USB 2.0 na parte frontal do equipamento.

1.4.1.5.5.2. Três portas USB 3.1, uma porta VGA e 1 porta RJ-45 para gerenciamento do equipamento, na parte traseira do equipamento.

1.4.1.5.6. Processador:

1.4.1.5.6.1. Cada nó deve contemplar no mínimo 02 (dois) processadores físicos, do mesmo modelo, sendo cada processador com as seguintes características:

1.4.1.5.6.2. 10 (dez), ou mais, núcleos de processamento (cores).

1.4.1.5.6.3. 20 (vinte), ou mais, threads.

1.4.1.5.6.4. Frequência base de 2.7GHz

1.4.1.5.6.5. Memória cache de 26.25 MB

1.4.1.5.7. Memória:

1.4.1.5.7.1. Cada nó da solução deve contemplar no mínimo 384 GB de memória RAM, padrão DDR5 ou superior, do tipo RDIMM, com suporte a detecção e correção de erros (Advanced ECC, SDDC, Chipkill ou tecnologia similar) e velocidade de operação de no mínimo 4.800 MHz. Os módulos de memória deverão possuir capacidade unitária mínima de 32GB.

1.4.1.5.7.2. Cada servidor da solução deve permitir a expansão da memória a pelo menos 8TB.

1.4.1.5.8. Armazenamento:

1.4.1.5.8.1. Cada nó deve ser fornecido com seu próprio sistema de armazenamento de dados.

1.4.1.5.8.2. Os nós deverão ter sua capacidade de armazenamento dimensionada de forma que a volumetria total do cluster seja de, no mínimo, 54TB (cinquenta e quatro Terabytes) líquidos considerando-se, fator de redundância 2 (RF-2) e que suporte a falha de um nó, não devendo considerar utilização de recursos de desduplicação, compressão de dados ou qualquer outra tecnologia de otimização de espaço, assim como todas as áreas recomendadas pelo fabricante (melhor prática) para perfeito funcionamento da solução. Serão aceitos como forma de comprovação da volumetria requerida ferramentas oficiais e em uso do fabricante para sizing dos equipamentos conforme todas as condições listadas acima.

1.4.1.5.8.3. Para acomodar o Sistema Operacional, cada nó deverá possuir 02 (dois) dispositivos padrão SSD de no mínimo 960 GB cada, configurados em RAID 1 a nível de hardware, podendo ser utilizadas as tecnologias SSD, M.2 NVMe;

1.4.1.5.9. Rede:

1.4.1.5.9.1. No mínimo 2 (duas) placas com 2 (duas) interfaces Ethernet cada, sendo a interface 10/25 Gbps.

1.4.1.5.9.2. Deverá vir acompanhado de 1 (um) transceiver SFP 1000Base-T (RJ45) para cada nó, cabo CAT6 3 (três) metros.

1.4.1.5.9.3. Possuir no mínimo 1 (uma) porta 1GbE para ser utilizada como interface de gerenciamento out-of-band.

1.4.1.5.9.4. O modelo da interface de rede ofertado deverá estar certificado/homologado para o hipervisor ofertado.

1.4.1.5.10. Placa Mãe:

1.4.1.5.10.1. Deve permitir a manipulação dos componentes removíveis da placa mãe sem o uso

de ferramentas e componentes hot-plug devem possuir identificação visual a fim de facilitar seu manuseio;

1.4.1.5.10.2. Possuir opção de criação de senha de acesso, senha de administrador ao sistema de configuração do equipamento.

1.4.1.5.10.3. Ser atualizável por software;

1.4.1.5.10.4. Controladora de vídeo integrada com, no mínimo, 16 MB.

1.4.1.5.11. Fonte de Alimentação:

1.4.1.5.11.1. Deve ser equipado de no mínimo 2 (duas) fontes, suportando o funcionamento do equipamento na configuração ofertada mesmo em caso de falha de uma das fontes;

1.4.1.5.11.2. Deve acompanhar cabo de alimentação para cada fonte de alimentação fornecida padrão C-14.

1.4.1.5.11.3. Potência deve ser suficiente para suportar o nó. Em caso de falha de uma das fontes, a fonte restante deve ser capaz de manter as condições elétricas e de potências adequadas para o funcionamento normal do servidor.

1.4.1.5.11.4. Suportar e operar nas faixas de tensão de entrada de 100-240 VAC em 60 Hz.

1.4.1.5.12. Sistema Operacional:

1.4.1.5.12.1. Deverá incluir licença Microsoft Windows Server Datacenter versão 2022, considerando o licenciamento total dos appliances de hiperconvergência.

1.4.1.6. Software Hiperconvergente

1.4.1.6.1. Deverá ser compatível com os hipervisores: Nutanix AHV, Microsoft Hyper-V e VMware ESXi. Não serão aceitos appliances que não funcionem os três hipervisores.

1.4.1.6.2. Para o Software Defined Storage (SDS), devem ser seguidas as melhores práticas para ambientes produtivos, em caso de recomendação explícita de um maior nível de proteção pelo fabricante;

1.4.1.6.3. Deverá ser fornecida unidade de subscrição de Software Hiperconvergente por núcleo de processamento (core) e suporte durante 60 (sessenta) meses na modalidade para Ambiente de Produção em operação 24x7, com início de atendimento em até 1h (uma hora) após abertura de chamados críticos;

1.4.1.6.4. O software hiperconvergente deverá incluir virtualização de infraestrutura (computação, rede e armazenamento) e o respectivo gerenciamento configurado de maneira a garantir alta disponibilidade e sem ponto único de falha.

1.4.1.6.5. O software hiperconvergente deverá permitir a configuração de um cluster com todos os equipamentos deste termo de referência, mesmo com as diferentes especificações de seus componentes internos, sendo permitida também a adição de novos equipamentos futuramente com novas gerações de processadores, diferentes configurações de discos, memória RAM e a inclusão de novos equipamentos com GPU para atender demandas de virtualização de desktops para equipe de engenharia.

1.4.1.6.6. Permitir a realização de snapshots e clones através da solução de armazenamento de dados definida por software (SDS), independente do hipervisor, utilizando algoritmo redirect-on-write para maior eficiência na utilização de storage bem como no tempo necessário para conclusão do snapshot ou clone.

1.4.1.6.7. Quando da inclusão online e não disruptiva de novos equipamentos com mais de uma camada de armazenamento (NVMe/SSD/HDD), o software deverá realizar a movimentação dos dados entre as camadas para favorecer o desempenho necessário aos dados mais acessados, garantindo a gestão do ciclo de vida dos dados (ILM) no nível do cluster;

1.4.1.6.8. A solução deverá permitir a configuração de domínios de disponibilidade de modo a tolerar a falha de equipamentos e racks. A falha de um disco não deve interromper ou impactar o funcionamento;

1.4.1.6.9. A CONTRATADA deverá possuir profissionais certificados pelo fabricante a nível profissional.

1.4.1.6.10. A subscrição de software deverá permitir a compressão de dados durante a sua ingestão e

após o seu armazenamento na camada de capacidade.

1.4.1.6.11. O SDS deverá permitir a desduplicação global dos dados, tanto na camada de desempenho quanto na camada de capacidade, de modo que até a replicação dos dados para outro cluster seja otimizada para reduzir o uso de banda.

1.4.1.6.12. Permitir a priorização do uso da camada de maior desempenho do storage para determinadas VMs e seus respectivos discos virtuais através da interface gráfica de gestão.

1.4.1.6.13. Deverá permitir a configuração de armazenamento através de volumes iSCSI para VMs em execução no cluster hiperconvergente e para aplicações externas ao cluster, inclusive baremetal.

1.4.1.6.14. Deverá permitir a realização de snapshots através do SDS com consistência para os dados da aplicação (application-consistent), tanto para VMs com sistema operacional Windows como para VMs com sistema operacional Linux, através de tecnologia VSS e semelhantes.

1.4.1.6.15. Permitir que o próprio administrador da máquina virtual realize a recuperação granular de arquivos sem a necessidade de envolvimento da equipe responsável pela gestão das cópias de segurança (backup).

1.4.1.6.16. Para aumento de segurança, a subscrição deverá permitir o bloqueio do cluster hiperconvergente para restringir o acesso administrativo ao hipervisor e SDS somente através do uso de chaves SSH, sem a utilização de senhas.

1.4.1.6.17. O software deverá permitir o uso da funcionalidade de segurança Windows Defender Credential Guard para isolamento das credenciais em máquinas virtuais com sistema operacional Windows, evitando ataques como Pass-the-Hash e Pass-The-Ticket;

1.4.1.6.18. O software hiperconvergente deverá permitir o emprego de tecnologias como vGPU para compartilhamento de GPU entre desktops virtualizados e GPU passthrough para aplicações de inteligência artificial e aprendizagem de máquina virtualizadas e conteinerizadas.

1.4.1.6.19. O software hiperconvergente deverá permitir o provisionamento automatizado, operações e a gestão do ciclo de vida de um cluster Kubernetes pronto para ambiente de produção.

1.4.1.6.20. A solução deverá permitir a gestão centralizada de múltiplos clusters no mesmo centro de dados e em centros distantes geograficamente para que seja possível gestão da infraestrutura, monitoramento de alertas e saúde destes clusters.

1.4.1.6.21. Deverá permitir a autenticação em nível empresarial utilizando Role Based Access Control (RBAC), sendo possível atribuir diferentes níveis de permissão para usuários e grupos de usuários.

1.4.1.6.22. Deverá permitir a integração com outras tecnologias através de APIs do tipo REST;

1.4.1.6.23. A interface de gerenciamento web deverá possuir uma ferramenta de busca contextualizada para acelerar as pesquisas na interface gráfica;

1.4.1.6.24. O fornecedor da solução deverá disponibilizar um portal de suporte para abertura de chamados, upload de logs e dados de diagnóstico relevantes para o chamado, acesso a documentação, base de conhecimento, download de atualizações, verificação de alertas relacionados à infraestrutura e compatibilidade de firmwares e softwares.

1.4.1.6.25. A solução deverá possuir uma ferramenta para automatizar e orquestrar todos os procedimentos necessários para atualização dos firmwares e softwares relacionados com um assistente para elaborar todo o planejamento e sequenciamento dos procedimentos de atualização.

1.4.1.6.26. Deverá oferecer um console unificado e baseado na nuvem para gerenciamento de multicloud híbrida.

1.4.1.6.27. O software também deverá:

1.4.1.6.27.1. Fator de redundância ajustável 2 ou 3.

1.4.1.6.27.2. Codificação de apagamento (EC-X).

1.4.1.6.27.3. QoS de armazenamento centrado em VM.

1.4.1.6.27.4. DR de múltiplos sites.

1.4.1.6.27.5. Failover com garantia de alta disponibilidade

1.4.1.6.27.6. Políticas de afinidade VM-Host.

1.4.1.6.27.7. Sobreposição de rede.

1.4.1.6.28. O Software hiperconvergente deve incorporar segurança em conformidade com padrões governamentais e internacionais de segurança e privacidade, NIST SP800-53, FIPS 140-2.

1.4.1.7. Documentação para avaliação:

1.4.1.7.1. Junto ao envio da proposta comercial, na sessão do pregão, a empresa licitante deverá enviar: datasheets, manuais ou guias de administração da plataforma hiperconvergente e software hiperconvergente, para fins de avaliação técnica, sob pena de desclassificação.

1.4.1.7.2. Junto ao envio da proposta comercial, na sessão do pregão, a empresa licitante deverá enviar documento comprobatório de ser parceira credenciada do fabricante da solução hiperconvergente, sob pena de desclassificação.

1.4.2. Switch Topo de Rack (ToR)

1.4.2.1. Cada switch deverá vir acompanhado de 1 (um) cabo do tipo DAC 100G para empilhamento com pelo menos 50cm.

1.4.2.2. Cada switch deverá vir com 18 (dezoito) transceivers SFP28 SR e 18 (dezoito) cordões ópticos multimodo de 5 (cinco) metros LC-LC OM3, sendo que os transceivers e cordões ópticos devem ser compatíveis e ter pleno funcionamento com o switch e com os appliances de hiperconvergência;

1.4.2.3. Deverá possuir 24 portas de 25GbE SFP28;

1.4.2.4. No mínimo 2 portas 100Gigabit Ethernet QSFP28;

1.4.2.5. Deve possuir capacidade de comutação de no mínimo 2.16 Tbps full duplex;

1.4.2.6. Deve possuir capacidade de throughput de no mínimo 1.42 Bpps full duplex;

1.4.2.7. Deve possuir fonte de alimentação interna redundante 110/220VAC;

1.4.2.8. As fontes de alimentação devem suportar hot-swap;

1.4.2.9. Deve possuir pelo menos 32MB de buffer de pacotes;

1.4.2.10. Deve possuir capacidade de no mínimo 280.000 (duzentos e oitenta mil) endereços MAC;

2.11. Deve suportar pelo menos 4096 VLANs;

1.4.2.12. Deve implementar Jumbo frames com tamanho de até 9216 bytes;

2.13. Deve implementar MSTP;

1.4.2.14. Deve implementar IEEE 802.3ad Link Aggregation Control Protocol (LACP);

1.4.2.15. Deve implementar IEEE 802.1w Rapid Reconfiguration of Spanning Tree;

1.4.2.16. Deve implementar IEEE 802.3x Flow Control;

1.4.2.17. Deve suportar dual stack IPv4/IPv6;

1.4.2.18. Deve implementar Listas de Controle de Acesso (ACL);

1.4.2.19. Deve implementar SNMPv2 e SSHv2;

1.4.2.20. Deve implementar DHCP Snooping, DHCP Server e DHCP Relay;

1.4.2.21. Deve implementar espelhamento de porta;

1.4.2.22. Deve permitir múltiplos arquivos de configuração;

1.4.2.23. Deve implementar LLDP.

1.4.2.24. Deve implementar NTP ou SNTP para sincronização de horário;

1.4.2.25. Deve permitir roteamento local entre VLANs utilizando interfaces virtuais ou SVIs;

1.4.2.26. Deve permitir a configuração de rotas estáticas usando endereços IPv4 e IPv6;

1.4.2.27. Deve possuir DHCP Server para IPv4 e IPv6;

1.4.2.28. Deve permitir a configuração de DHCP Relay;

1.4.2.29. Deve implementar PBR (Policy-Based Routing) para IPv4 e IPv6;

1.4.2.30. Deve permitir priorização de tráfego usando 8 (oito) filas de priorização por porta;

1.4.2.31. Deve permitir priorização de tráfego baseado no padrão IEEE 802.1p e no campo DSCP do protocolo Diffserv;

1.4.2.32. Deve implementar protocolo de VXLAN;

1.4.2.33. Deve implementar mecanismo EVPN-VXLAN em L2VPN e L3VPN sobre IP e MPLS;

1.4.2.34. Deve implementar protocolo de roteamento BGPv4 e Extensões Multiprotocolos MP-BGP;

1.4.2.35. Deve implementar mecanismo de detecção de falhas bidirecionais na convergência (BFD) em pelo menos nos seguintes protocolos: OSPF, BGP e VRRP em IPv4 e IPv6;

1.4.2.36. Deve implementar mecanismo de Graceful Restart para os protocolos OSPF ou BGP;

1.4.2.37. Deve implementar pelos menos os seguintes métodos para configuração das filas de priorização: ponderada, prioridade estrita e ambas combinadas;

1.4.2.38. Implementar priorização de tráfego baseado em porta física, protocolo IEEE 802.1p, endereços IP de origem e destino e portas TCP/UDP de origem e destino;
1.4.2.39. Deve permitir a configuração de Rate Limiting de entrada;
1.4.2.40. Deve permitir a configuração de Rate Shaping de saída;
1.4.2.41. Deve permitir o envio de mensagens de syslog a pelo menos 2 servidores distintos;
1.4.2.42. Deve ser permitida a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;
1.4.2.43. O equipamento deverá ser homologado pela Agência Nacional de Telecomunicações (ANATEL).

1.4.3. Solução de Backup

1.4.3.1. Appliance de Backup

1.4.3.1.1. Características:
1.4.3.1.1.1. Deverá ser fornecido um sistema inteligente de armazenamento de backup em disco, que se entende como uma solução com o propósito específico de armazenamento de backup de dados, com criptografia, compactação, desduplicação e replicação dos dados desduplicados ativa;
1.4.3.1.1.2. Deverá utilizar arquitetura Scale-up, ou Scale-out, de acordo com as especificações técnicas descritas;
1.4.3.1.1.3. Deve constar no site oficial do fabricante (referenciando o link público), como um appliance de propósito exclusivamente para o de backup em disco, não sendo aceitas soluções alternativas para atendimento aos requisitos obrigatórios requeridos;
1.4.3.1.1.4. Deve ser composto exclusivamente por hardware e software (microcódigo ou firmware) do mesmo fabricante, não serão aceitas soluções montadas especificamente para esse certame, composições de soluções em regime de OEM, nem equipamentos usados, remanufaturados e de demonstração;
1.4.3.1.1.5. Não serão aceitas soluções alternativas, definidas por Software (software defined storage ou virtual appliances), baseadas em Windows Storage Server; composições baseadas em NAS gateway ou similares, montadas para atendimento aos requisitos obrigatórios requeridos.
1.4.3.1.1.6. Deverá ser novo, de primeiro uso, da linha de equipamentos (modelos) mais recentemente anunciada pelo fabricante e em linha de fabricação, sem previsão de EOSL (end of Service life) anunciado pelo fabricante durante toda vigência do período de suporte contratado
1.4.3.1.1.7. O appliance deve ser entregue com todos os trilhos, cabos, conectores, manuais de operação e quaisquer outros componentes que sejam necessários à instalação, customização e plena operação;
1.4.3.1.1.8. Deve permitir a utilização de todas as funcionalidades, tecnologias e recursos especificados, em sua totalidade, de maneira perpétua, irrestrita e sem necessidade de licenciamento ou ônus adicional. Caso seja necessária alguma licença adicional para tal, ela deverá ser parte integrante da proposta da licitante.;
1.4.3.1.1.9. Deverá ser fornecido com licenças na modalidade de uso perpétuo para todo o completo atendimento das especificações técnicas dos equipamentos, ou seja, os equipamentos deverão continuar a operar normalmente mesmo após o término do período de manutenção e assistência técnica contratado;
1.4.3.1.1.10. Todas as licenças necessárias para o pleno funcionamento do sistema inteligente de armazenamento de backup deverão ser parte integrante da proposta do licitante, garantindo a plena utilização de todos os recursos requeridos sem ônus adicional a CONTRATENTE.
1.4.3.1.1.11. Deve considerar no sistema de cálculo BASE 10, onde 1TB = 1000GB para todos os requerimentos capacidade e/ou performance, relativos ao Subsistema de Backup em Disco proposto;
1.4.3.1.1.12. Deverá ser entregue com todos os trilhos padrão rack 19”, e respectivos cabos, conectores, manuais de operação e quaisquer outros componentes que sejam necessários à instalação, customização e plena operação no ambiente da CONTRATANTE;

1.4.3.1.2. FUNCIONALIDADES

1.4.3.1.2.1. Deve permitir a execução de processos de backup e restore em paralelo;
1.4.3.1.2.2. Deve suportar acessos de leitura e gravação simultâneo, pelos protocolos padrões de mercado: CIFS (SMB2, SMB3 ou superiores), NFS (V3 e V4 ou superiores) e OST;
1.4.3.1.2.3. Deve possuir interface WEB HTTPS para gerenciamento do sistema de armazenamento de backup;
1.4.3.1.2.4. Deve possuir desduplicação global, mesmo que o armazenamento esteja dividido em volumes lógicos, sendo capaz de identificar dados duplicados de backups de diferentes origens dentro de um mesmo sistema de modo a maximizar a taxa de desduplicação e garantindo que os dados retidos sejam gravados uma única vez;
1.4.3.1.2.5. Deve suportar que a desduplicação seja realizada juntamente com as operações de backup e restauração, tornando desnecessária uma janela dedicada para sua execução;
1.4.3.1.2.6. Deve implementar mecanismos para validação da consistência dos dados desduplicados armazenados, garantindo que eles estejam íntegros durante backups, restaurações e replicações, devendo reparar, automaticamente, dados que não estejam consistentes com as rotinas executadas. O mecanismo deve ser nativo do equipamento, não sendo aceitos scripts para atendimento deste item;
1.4.3.1.2.7. Deve permitir replicar os dados através de rede IP (WAN/LAN);
1.4.3.1.2.8. Deve permitir replicar os dados de backup em site remoto de forma assíncrona, previamente desduplicados, entre sistemas semelhantes do mesmo fabricante, trafegando somente o bloco desduplicado e consequentemente, reduzindo assim o consumo do link de comunicação;
1.4.3.1.2.9. Deve permitir a implementação de topologias de replicação, como 1:1, 1:N, N:1 e o cascateamento de equipamentos sem quaisquer custos adicionais;
1.4.3.1.2.10. Deverá possibilitar a integração com plataformas de armazenamento em nuvem pública para propósitos de replicação. Entende-se como integração a possibilidade de replicação dos dados de backup para uma infraestrutura em nuvem pública, podendo esta ser fornecida pelo menos por dois provedores de nuvem, como AWS e Azure em modalidade licenciamento por subscrição ou perpétua. O licenciamento desse item não faz parte deste certame;
1.4.3.1.2.11. Deve possuir suporte aos protocolos de monitoramento SNMP e Syslog;

1.4.3.1.3. ARQUITETURA

1.4.3.1.3.1. O sistema ofertado deverá possuir uma arquitetura do tipo "scale-up" ou do tipo "scaleout" assegurando escalabilidade vertical ou horizontal. Consequentemente, não serão aceitas ofertas de sistemas baseados em federação ou cluster de equipamentos de menor porte, se o conjunto do repositório de armazenamento não for capaz de efetuar desduplicação global dos dados retidos entre os dispositivos. Gateways ou composições desenvolvidas e fabricadas exclusivamente para fins de atendimento do objeto do edital não serão aceitas em hipótese alguma;
1.4.3.1.3.2. Para soluções com arquitetura Scale-Out:
1.4.3.1.3.2.1. Deve permitir a interconexão com outros subsistemas de armazenamento de backup em disco do mesmo fabricante de forma online, a fim de ampliar o desempenho e respectiva capacidade de armazenamento de forma linear;
1.4.3.1.3.2.2. Deverá possuir a funcionalidade de desduplicação global, ou seja, somente os blocos, segmentos e/ou bytes distintos de dados deverão ser gravados considerando toda área de retenção ofertada e expansões futuras na solução proposta;
1.4.3.1.3.2.3. Deverá operar em modo de alta-disponibilidade para as tarefas de backup, em modo ativo-ativo, com balanceamento de carga permitindo que, na falha de uma das unidades do sistema de armazenamento em disco, as atividades de backup, possam ser automaticamente redirecionadas para outro sistema de armazenamento do

mesmo conjunto;

1.4.3.1.3.3. Para soluções com arquitetura Scale-Up;

1.4.3.1.3.3.1. O subsistema de backup em disco deverá possuir no mínimo duas controladoras, implementadas em alta-disponibilidade, de forma “ativo-ativo” com balanceamento de carga ou ativo-passivo para as tarefas de backup, permitindo que na falha de uma controladora, os Jobs de backup possam ser automaticamente redirecionadas para a controladora remanescente do mesmo conjunto;

1.4.3.1.3.3.2. Deve possibilitar a desduplicação global para toda área de retenção de dados, sendo esta, distribuída em uma ou mais de uma controladora ativa funcionando como um único equipamento, desconsiderando soluções alternativas como federação ou similares;

1.4.3.1.3.4. Deve possuir recursos de tolerância a falhas de, pelo menos, discos, fontes de alimentação e ventiladores;

1.4.3.1.3.5. Deve possuir mecanismos que proteja a solução contra inconsistências dos dados, mesmo em casos de interrupção abrupta do fornecimento de energia ou desligamento acidental;

1.4.3.1.3.6. Deve possuir tecnologia para proteger a cache de escrita, evitando a perda de dados em eventos de falha elétrica;

1.4.3.1.3.7. Deve ser entregue com arranjos de discos rígidos do tipo RAID-6, RAID-DP ou similar para os discos destinados ao armazenamento de dados de backup, permitindo tolerar a falha de até 2 (dois) discos rígidos, contando com ao menos 1 disco de hot-spare para cada RAID group;

1.4.3.1.3.8. Deve possuir discos rígidos hot-pluggable e hot-swappable, permitindo substituição sem necessidade interrupção do funcionamento da solução;

1.4.3.1.3.9. Deve possuir recursos de monitoramento remoto pelo fabricante, tal como notificação do tipo Call-Home, para verificação proativa de componentes de hardware em situação de falha ou pré-falha;

1.4.3.1.4. COMPATIBILIDADE

1.4.3.1.4.1. O modelo do equipamento ofertado, deve ser homologado como Backup Appliance para o Veeam B&R, mediante consulta na matriz de compatibilidade do fabricante do software (https://www.veeam.com/alliance-partner-technical-programs.html), e em pelo menos mais um dos softwares descritos abaixo:

1.4.3.1.4.2. Veritas NetBackup (https://sort.veritas.com/DocPortal/pdf/NB_100_HCL) e Commvault (https://www.commvault.com/supported-technologies);

1.4.3.1.4.3. Deve permitir que a aplicação Oracle (RMAN) realize backups do tipo Stream Based e “database dump”, e a aplicação Microsoft SQL realize backups do tipo “database dump” diretamente para o equipamento, via CIFS e NFS, sem utilizar o software de backup para evitar, assim, o consumo de suas licenças e sem a necessidade de licenciar os volumes (TBs) ou os servidores de banco de dados (CPU, Tier, Core) junto ao software de backup. Caso para a implementação desta funcionalidade seja necessário o fornecimento de licenciamento adicional, e as respectivas licenças deverão fazer parte da proposta da licitante considerando toda capacidade requerida;

1.4.3.1.5. SEGURANÇA

1.4.3.1.6. Deve possuir integração com o Microsoft Active Directory, para autenticação e definição de perfis de acesso;

1.4.3.1.7. Deve possuir criptografa dos dados armazenados em padrão FIPS 140-2, utilizando no mínimo os algoritmos 256-bits AES.

1.4.3.1.8. Para o armazenamento local, o mesmo deverá ser provido através de SED drives. Caso o fabricante implemente a criptografia através de software nas controladoras do subsistema de backup, deverá ser fornecido, adicionalmente ao requerido, 30% a mais de

performance de taxa de transferência considerando o overhead ocasionado na solução.

1.4.3.1.9. Caso a solução proposta não suporte a replicação dos dados criptografados, deverão ser fornecidos adicionalmente a solução proposta, um appliance baseado em hardware que possibilite a implementação de TUNNELING entre os dados de origem e destino, garantindo a segurança

1.4.3.1.10. Deverá possuir suporte a TLS, SSH e Kerberos;

1.4.3.1.11. Deve permitir a configuração de duplo fator de autenticação para acesso ao sistema, via integração com soluções de senha descartável (senha de uso único, em inglês: One-time password - OTP), tais como Google Authenticator, Microsoft Authenticator ou similares:

1.4.3.1.11.1. Caso o equipamento requeira um dispositivo/sistema 2FA/OTP específico que necessite de licenciamento, hardwares, VMs e/ou infraestrutura próprios – por exemplo: Common Access Card (CAC)/Personal Information Verification (PIV) cards, sistemas de OTP/tokenização licenciados, etc. – esses componentes (hardwares, VMs, softwares, licenças, serviços, etc.) devem ser fornecidos com a solução para, no mínimo, 10 usuários. Apenas será admitido o fornecimento deste recurso através de subscrição (por período igual ou superior a garantia solicitada no item) quando inexistir a modalidade perpetua no modelo de licenciamento do fornecedor. Em nenhuma hipótese esse recurso poderá ser instalado em máquinas virtuais no ambiente de tecnologia existente do CONTRATANTE, uma vez que tal possibilidade compromete o objetivo final de segurança dos dados armazenados em backup, dado que um ataque a infraestrutura de produção comprometeria o sistema de proteção 2FA/OTP. As características de licenciamento de software e respectivos hardwares/infraestruturas adicionais, deverão acompanhar a proposta do licitante, bem como os requisitos de suporte e SLA especificados neste edital devem ser mantidos, inclusive para esse recurso;

1.4.3.1.12. Deve possuir recursos de proteção contra ataques cibernéticos, notadamente contra perda de dados de backup em disco por ataque de ransomware, bem como por ataque interno por usuário mal intencionado, com as seguintes características:

a - Imutabilidade: garantir que os dados de backups retidos no repositório não possamser alterados ou apagados. Deve ser aplicado de maneira automática e transparente, independentemente do software/utilitário de backup, sem requerer scripts, ações e intervenções manuais, e intervalo mínimo para a aplicação do recurso.

b - Dupla Autorização: garantir que ações críticas que possam comprometer a segurançada solução e dos dados somente sejam aplicadas mediante a aprovação de um segundo usuário, com papel específico de aprovador, suportando aprovação no mínimo das seguintes ações: remoção dos repositórios/compartilhamentos/partições; quebra da replicação; modificação, desativação e exclusão das configurações de proteção contra ransomware; e criação e modificação de novos usuários aprovadores;

c - Recurso nativo de atraso (air-gap): garantir que os dados desduplicados no repositórioestejam invisíveis da superfície de ataque, isto é, não poderão ser diretamente acessados através da rede, nem pelo software/utilitário de backup. O uso de protocolos/APIs proprietários não será aceito isoladamente para atendimento a este item, dado que tal recurso não protege situações em que o software/utilitário de backup fique sob domínio do atacante, evitando impedir ataques internos por usuários malintencionados. Esse recurso deve ser implementado através de mecanismos próprios e internos do equipamento, não sendo aceito snapshots.

1.4.3.1.13. Caso o equipamento ofertado não atenda integralmente um ou mais dos requisitos de segurança detalhados nos itens a, b e c acima, será admitido o fornecimento de um equipamento adicional que terá a finalidade específica de armazenar uma réplica segura dos dados desduplicados contidos no equipamento de backup primário, utilizando-se de uma infraestrutura isolada através de mecanismos de rede. Tal equipamento deverá respeitar as mesmas características de modelo, tamanho, escalabilidade e desempenho do equipamento primário/principal, bem como todo o licenciamento e serviços pertinentes devem ser contemplados na proposta da LICITANTE para que o recurso seja entregue completamente funcional.

1.4.3.1.14. CARACTERÍSTICAS ESPECIFICAS DE CAPACIDADE, DESEMPENHO E CONECTIVIDADE

1.4.3.1.14.1. Deve atender aos requerimentos descritos nos itens anteriores que descrevem as características gerais, funcionalidades, compatibilidade, arquitetura e segurança;

1.4.3.1.14.2. Deve possuir no mínimo 50TB (cinquenta terabytes) úteis em base 10 (1TB=1000GB), sem considerar taxa de desduplicação, compressão, perdas com formatação e área necessária para o sistema do equipamento);

1.4.3.1.14.3. Deve possuir pelo menos 2 (duas) interfaces de rede 25GbE (vinte e cinco gigabit ethernet) para conexão com switch LAN (interconnect) por meio de conector SFP28 (optico) para Backups executados via LAN. Deverão ser entregues cabos LC-LC OM3 com no mínimo 5 metros de comprimento por porta.

1.4.3.1.14.4. Deve possuir pelo menos 2 (duas) interfaces de rede 1 GbE (um gigabit Ethernet) para conexão com switch LAN (interconnect) por meio de conector UTP CAT6 para gerenciamento. Os conectores devem ser fornecidos em conjunto com o equipamento;

1.4.3.1.14.5. Deve possuir pelo menos 1 (um) Porta IPMI/iLO/iDRAC ou similar;

1.4.3.1.14.6. Deve possuir taxa de transferência de, no mínimo, 6TB/hora (seis terabytes por hora) para operações de backup desconsiderando qualquer ganho com compressão e deduplicação na origem (cliente e servidor de backup) ou instalação de qualquer agente no servidor ou cliente de backup.

1.4.3.1.14.7. Deve possuir criptografia certificada FIPS 140-2 utilizando no mínimo 256-bit AES baseada em hardware. Caso a criptografia seja baseada em software, o desempenho (taxa de transferência) do sistema deve ser 30% maior ao requisitado no item anterior, sem utilizar desduplicação na origem para esse cálculo. Todas as licenças e componentes necessários a essa função devem ser fornecidos em conjunto com a solução.

1.4.3.1.14.8. Deve fornecer interfaces adicionais, caso seja indicado pelas melhores práticas do fabricante da solução, para atendimento dos requerimentos de desempenho;

1.4.3.1.14.9. Toda parte de conectividade de rede como switches, roteadores, etc, será provido pela CONTRATANTE.

1.4.3.1.15. SERVIÇOS DE GARANTIA E SUPORTE TECNICO DO SISTEMA SEGURO DE ARMAZENAMENTO DE BACKUP EM DISCO DO TIPO “APPLIANCE”

1.4.3.1.16. GARANTIA

1.4.3.1.16.1.O prazo de garantia contratual dos bens/serviços, complementar à garantia legal prevista pelo art.26 da Lei Federal n°. 8.078 de 1990 (Código de defesa do Consumidor-CDC) é de no mínimo 60 (sessenta) meses ou pelo prazo fornecido pelo fabricante, se superior, contando a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

1.4.3.1.17. SUPORTE

1.4.3.1.17.1. A CONTRATANTE poderá efetuar um número ilimitado de chamados técnicos, durante o período da garantia, para correção de problemas relativos ao uso e aplicações dos equipamentos, software e suas funcionalidades.

1.4.3.1.17.2. A CONTRATADA deverá apresentar na entrega do objeto declaração de garantia de no mínimo 60 (sessenta) meses, informando que será adquirido todas peças ou softwares do fabricante da solução necessários ao perfeito funcionamento do objeto contratado.

1.4.3.1.17.3. Durante o período de garantia o Fornecedor deve se comprometer com a execução de atividades de atendimento em garantia e correções da solução ofertada, visando eliminar erros detectados nos produtos que impeçam seu pleno funcionamento de acordo com as especificações listadas neste documento. Este compromisso deve ser demonstrado mediante documento declaração do

fabricante;

1.4.3.1.17.4. Os equipamentos deverão ser garantidos no Brasil, sem itens restritivos, tanto para o hardware como para o software, com atendimento em português pelo menos durante o horário comercial;

1.4.3.1.17.5. O fornecedor da solução irá fornecer as últimas versões dos softwares utilizados pelos equipamentos, contendo correções de bugs, atualizações ou novas funcionalidades suportadas pelo equipamento em questão, bem como as respectivas licenças de uso de acordo com o especificado/exigido pelo fabricante da solução.

1.4.3.1.17.6. O Fabricante da solução deverá fornecer drivers e firmware, incluindo atualizações de versões e pequenas atualizações de release e reparos de defeitos (bug fixing patches) pelo período da garantia contratada.

1.4.3.1.17.7. Para garantir o atendimento dos serviços em garantia dos produtos instalados, a contratada deverá disponibilizar suporte por meio de um Centro de Suporte Técnico reconhecido pelo fabricante da solução oferecida, podendo ser uma Assitência Técnica Autorizada ou um Revendedor Credenciado.

1.4.3.1.17.8. O suporte deve contemplar a função de "call home" do fabricante, através de linha VPN ("Virtual Private network") ou acesso seguro a para a central do fabricante, visando permitir diagnóstico remoto em caso de erros/defeitos e abertura automatizada de chamados

1.4.3.1.17.9. Os serviços de suporte técnico ao produto deverão incluir, dentre outros:

1.4.3.1.17.10. Orientações sobre uso, procedimentos, configuração e instalação do software ofertado;

1.4.3.1.17.11. Questões sobre compatibilidade e interoperabilidade do produto ofertado (hardware e software);

1.4.3.1.17.12. Acompanhamento e orientação dos procedimentos específicos de recuperação de dados da solução ofertada em casos de ataques cibernéticos que exijam a recuperação de dados a partir dos dados protegidos através do recurso air-gap na solução;

1.4.3.1.17.13. Orientações para identificar a causa de uma falha de hardware;

1.4.3.1.17.14. Orientação quanto às melhores práticas para implementação do hardware adquirido;

1.4.3.1.17.15. Apoio para execução de procedimentos de atualização para novas versões do microcódigo instalado.

1.4.3.1.17.16. SUPORTE TÉCNICO NÍVEL 2

1.4.3.1.17.16.1. A CONTRATADA deverá fornecer juntamente com a solução de armazenamento de backup em disco acesso a um engenheiro de suporte nomeado de 2º nível do fabricante (nível onde o analista de suporte é qualificado para atuar diretamente no problema, sem necessidade de triagem prévia), que atuará como ponto único de contato para fornecer assistência avançada de forma remota em horário comercial

1.4.3.1.17.16.2. A função do suporte técnico nível 2, devidamente qualificado na solução ofertada, deve estar disponível pelo mesmo período do suporte contratado e deve ser fornecido pelo próprio fabricante da solução ofertadaatravés da Contratada;

1.4.3.1.17.16.3. Deve coordenar os eventos de manutenção dos equipamentos de acordo com a janela de manutenção da CONTRATANTE;

1.4.3.1.17.16.4. Deve possuir interlocução direta com a engenharia e backoffice do fabricante do hardware para escalonamento e acompanhamento de chamados;

1.4.3.1.17.16.5. Deve permitir que a CONTRATANTE demande, a qualquer tempo, durante o período de garantia, avaliações destinadas a melhorar a eficiência operacional, quando considerado necessário pela CONTRATANTE.

1.4.3.1.17.16.6. O suporte nível 2 será responsável pela análise da solução proposta e pelo engajamento dos recursos necessários para a solução dos problemas encontrados, além de realizar o monitoramento dos chamados técnicos abertos para garantir o

correto endereçamento.

1.4.3.1.17.16.7. Caso este engenheiro de suporte esteja temporariamente indisponível, será dada a opção do chamado ser redirecionado para um outro engenheiro de suporte também de 2º nível disponível naquele momento. O engenheiro de suporte nível 2 do fabricante deve, adicionalmente, realizar durante todo o período de garantia as seguintes atividades: atualização da solução de armazenamento de backup, verificações proativas junto ao CONTRATANTE, esclarecimento de dúvidas técnicas e apoio em atividades de revisão e alteração de configurações do dia a dia, análise e suporte na solução de problemas de “performance” e “tuning” das configurações do firmware ofertado;

1.4.3.1.17.16.8. O suporte nível 2 deverá estar disponível para prestar esclarecimentos de dúvidas técnicas ou operacionais (operação do ambiente, degradação de performance, etc.) referente a solução ofertada, durante todo o período da garantia;

1.4.3.1.17.16.9. Caso a CONTRATADA não consiga atender ao nível de suporte exigido com recurso nomeado de 2º nível, deverá fornecer serviços adicionais como forma de atendimento, desde que seja do próprio fabricante e seja disponibilizado recurso humano certificado tecnicamente na solução, no qual será ponto único de contato para todas as questões relacionadas ao suporte técnico mencionados anteriormente, incluindo abertura e acompanhamento de ponta-a-ponta dos casos de suporte, assim como das demais atividades.

1.4.3.1.17.16.10. Caso qualquer serviço anteriormente descrito não esteja disponível na oferta padrão do fabricante, a CONTRATADA deverá contemplar em sua proposta o fornecimento de, no mínimo, 4 atendimentos mensais, com profissional do fabricante, que seja qualificado para a execução dos serviços descritos nos requisitos obrigatórios do edital.

1.4.3.2. Software de Backup

1.4.3.2.1. Cada licença de software deverá corresponder a no mínimo 40 (quarenta) cargas de trabalho (instâncias), e esta licença poderá ser utilizada em máquinas físicas, virtuais, bancos de dados, entre outras aplicações e sistemas;

1.4.3.2.2. As licenças deverão possuir vigência de 60 (sessenta) meses, com cobertura de suporte e assistência técnica oficial de sua fabricante, com cobertura de atendimento 24x7x365 e disponibilidade de contato técnico através de sistema web e telefone.

1.4.3.2.3. COMPATIBILIDADE COM APLICAÇÃO

1.4.3.2.3.1. A solução ofertada deverá ser compatível nativamente com as seguintes tecnologias:
1.4.3.2.3.2. VMware vCenter e vSphere ESXi versões 6.0 ou superiores.
1.4.3.2.3.3. VMware vCloud Director versões 9.7 ou superiores.
1.4.3.2.3.4. Microsoft System Center Virtual Machine Manager e Hyper-V 2012 ou superiores.
1.4.3.2.3.5. Nutanix AHV 5.11 ou superiores.
1.4.3.2.3.6. Nuvem da Amazon Web Services (AWS) EC2 e Microsoft Azure VM.
1.4.3.2.3.7. Microsoft Active Directory 2012 ou superiores.
1.4.3.2.3.8. Microsoft Exchange 2013 ou superiores.
1.4.3.2.3.9. Microsoft SharePoint 2013 ou superiores.
1.4.3.2.3.10. Microsoft File Server Failover Cluster 2016 ou superiores.
1.4.3.2.3.11. Microsoft SQL Server 2014 ou superiores.
1.4.3.2.3.12. Oracle Database 12g ou superiores.
1.4.3.2.3.13. MySQL 5.6 ou superiores.
1.4.3.2.3.14. PostgreSQL 12 ou superiores.
1.4.3.2.3.15. Suportar proteção dos seguintes sistemas operacionais:
1.4.3.2.3.16. Microsoft Windows Server 2012 ou superiores.
1.4.3.2.3.17. Microsoft Windows 7 SP1 ou superiores.
1.4.3.2.3.18. CentOS Linux 7 ou superiores.
1.4.3.2.3.19. Debian Linux 9 ou superiores.
1.4.3.2.3.20. Red Hat Enterprise Linux 7 ou superiores
1.4.3.2.3.21. Oracle Linux 7 ou superiores

1.4.3.2.3.22. SUSE Linux Enterprise Server 15ou superiores.
1.4.3.2.3.23. Ubuntu 16.04 LTS ou versões LTS superiores.
1.4.3.2.3.24. Suportar a recuperação granular dos dados dos seguintes sistemas de arquivos do tipo: Btrfs, ext3, ext4, HFS, HFS+, JFS, ReiserFS, XFS, FAT32, NTFS e ReFS.

1.4.3.2.4. COMPATIBILIDADE COM INFRAESTRUTURA

1.4.3.2.4.1. Possuir recurso para possibilitar a reconstrução do catálogo dos dados de backup armazenados em disco e fita.
1.4.3.2.4.2. Suportar desduplicação a nível de blocos, em volumes apresentados através de DAS (Direct Attached Storage) e SAN (Storage Area Network) e em compartilhamento de rede NAS, via protocolos SMB e NFS.
1.4.3.2.4.3. Suportar desduplicação de dados no servidor de armazenamento (target deduplication), de forma que o servidor de backup descarte blocos repetidos de clientes, evitando assim o armazenamento de blocos redundantes.
1.4.3.2.4.4. Suportar desduplicação de dados na origem (source deduplication), de forma que sejam enviados apenas novos blocos de dados criados e/ou modificados apartir da última cópia
de segurança.
1.4.3.2.4.5. Permitir armazenar cada máquina virtual em um arquivo de backup distinto ao armazenar cópias de segurança em Appliances de Desduplicação, suportando no mínimo os seguintes modelos de equipamento: DellEMC Data Domain (powerprotect), Exagrid, HPE StoreOnce e Quantum DXi;
1.4.3.2.4.6. Deve possuir a capacidade de gerenciar software de snapshot de storages de outros fabricantes, tais como DellEMC, IBM, NetApp, HPE e Pure Storage, com o intuito de automatizar o processo de agendamento de cópias “snapshot” e montagem no servidor de backup “off-host”;
1.4.3.2.4.7. Suportar proteção de dados de dispositivos de Storage NAS (Network Attached Storage) via protocolo NDMP (Network Data Management Protocol) versão 4.
1.4.3.2.4.8. Suportar qualquer tecnologia utilizada na infraestrutura de armazenamento como destino das cópias de segurança: S3, DAS, NAS e SAN, sem prejuízos das demais funcionalidades suportadas pelo software.
1.4.3.2.4.9. Paralelizar a gravação de dados de uma rotina de backup em diferentes caminhos pertencentes à vários dispositivos de armazenamento.
1.4.3.2.4.10. Permitir a gravação serial e simultânea de várias rotinas de backup, provenientes de clientes distintos, em um único caminho pertencente a um dispositivo de armazenamento (funcionalidade conhecida como multiplexação).
1.4.3.2.4.11. Permitir exportar o conteúdo de backup para mídia removível, possibilitando o transporte físico de dados até o destino.
1.4.3.2.4.12. Ser flexível e escalável, permitindo sua instalação, configuração e uso em sites remotos interligados ao site principal através da WAN ou através de LAN.
1.4.3.2.4.13. Prover recursos de desduplicação e compressão tanto no site principal como nos sites remotos.
1.4.3.2.4.14. Possuir interface gráfica e/ou web, capaz de gerenciar um ou mais sites de forma centralizada.
1.4.3.2.4.15. Suportar o armazenamento local de dados.
1.4.3.2.4.16. Suportar o envio das cópias de segurança para unidades de fita LTO Ultrium 5 e superiores.
1.4.3.2.4.17. Suportar meios de otimização do consumo de fita, através do agrupamento de dados que estão espalhados em diversas fitas com baixa porcentagem de utilização, movendo esses dados para uma nova fita ou através de políticas que garantam uma melhor consolidação de backups e permitam a cópia dos backups desduplicados e comprimidos para a fita, sem a necessidade de reidratação dos dados.
1.4.3.2.4.18. Permitir cópias adicionais do backup principal com funcionalidade de criar múltiplas cópias em fitas.

1.4.3.2.4.19. Suportar a gravação em bibliotecas de fitas automatizadas.

1.4.3.2.4.20. Permitir o gerenciamento de fitas armazenadas, tanto internamente em bibliotecas de fita, quanto em cofres externos, permitindo o registro das movimentações de fitas entre as bibliotecas de fita e cofres externos.

1.4.3.2.4.21. Suportar a gravação em fitas WORM (Write Once Read Many).

1.4.3.2.4.22. Suportar as operações de backup e restauração em paralelo.

1.4.3.2.4.23. Possibilitar o backup e a restauração das informações em disco e fita.

1.4.3.2.4.24. A solução deverá permitir a construção de um repositório de armazenamento de backup com escalabilidade horizontal, garantindo uma arquitetura híbrida entre nuvem privada e nuvem pública. Deverá permitir o uso simultâneo, com o propósito de criar uma entidade virtual de armazenamento, de storages, appliances de desduplicação e arquiteturas de nuvem (S3 ou similares);

1.4.3.2.4.25. A solução deverá permitir que o repositório de armazenamento escalável seja composto, concomitantemente, por armazenamento direto em Windows/Linux (SAN ou DAS), compartilhamentos de rede (NAS), equipamentos específicos para deduplicação (PBBA) e armazenamento de Objetos (S3 e HTTP) em nuvem pública e privada;

1.4.3.2.4.26. A solução deverá permitir elencar, por características de desempenho dos repositórios, distintos níveis de armazenamento com o propósito de garantir estabilidade nos processos de backup e restauração de dados;

1.4.3.2.4.27. A solução deverá permitir a escolha do armazenamento contínuo das imagens de backup, de modo que um ciclo de backup possa estar presente em um único elemento da infraestrutura compartilhada (integralmente em um appliance de desduplicação), bem como em múltiplos elementos da infraestrutura compartilhada (backups completos em um appliance de deduplicação e backups incrementais em compartilhamentos NAS ou S3);

1.4.3.2.4.28. A solução dever validar diariamente, de modo automático, o estado dos distintos elementos de armazenamento que compõem o repositóriocompartilhado. A solução deverá validar o status de cada elemento, informando se eles estão online ou não, se os movimentadores de dados estão estáveis e qual o espaço de armazenamento remanescente no repositório compartilhado global.

1.4.3.2.5. REPLICAÇÃO DE DADOS

1.4.3.2.5.1. Permitir replicação de uma origem para múltiplos destinos.

1.4.3.2.5.2. Suportar a replicação das cópias de segurança para diversos sites remotos, permitindo ainda que a restauração dos dados seja feita através das cópias armazenadas remotamente.

1.4.3.2.5.3. Permitir replicação e consolidação de dados de múltiplas origens para um destino central.

1.4.3.2.5.4. Permitir o uso de diferentes políticas de retenção de dados nos repositórios de origem e destino durante o processo de replicação.

1.4.3.2.5.5. Possuir mecanismos que evitem o aumento do tempo de resposta dos datastores de produção, monitorando a latência dos datastores e reduzindo as atividades de backup quando um limite configurado for atingido, evitando a sobrecarga nos sistemas de armazenamento dos ambientes de virtualização vSphere e Hyper-V;

1.4.3.2.5.6. Possuir capacidade de realizar a replicação de máquinas virtuais VMware e Hyper-V localmente e remotamente em outro Cluster, realizando clones ou snapshots com proteção contínua dos dados por máquina virtual.

1.4.3.2.5.7. Deverá suportar a replicação remota a fim de replicar os dados das máquinas virtuais entre soluções de armazenamento distintas, inclusive de diferentes fabricantes.

1.4.3.2.6. PROTEÇÃO DE DADOS E APLICAÇÕES

1.4.3.2.6.1. Suportar a proteção completa de servidores físicos, workstations, desktops e notebooks com backups a nível de imagem, tanto em nível de arquivos, quanto em nível de volumes.

1.4.3.2.6.2. Permitir a criação de imagens de recuperação inicializáveis dos backups de Linux e Windows para recuperação de desastres (funcionalidade conhecida como Bare-Metal Restore) de forma nativa e sem a utilização de software de terceiros.

1.4.3.2.6.3. Suportar a recuperação desses backups diretamente em um ambiente virtual VMware vSphere, Microsoft Hyper-V e Nutanix AHV de maneira instantânea, realizando a conversão P2V (físico para virtual) e inicializando diretamente dos arquivos de backup, sem a necessidade de esperar a conclusão da restauração para ter acesso à máquina ou agendamento de rotinas periódicas para isso.

1.4.3.2.6.4. Suportar a restauração do sistema inteiro para equipamentos com o mesmo hardware e para equipamentos com hardware diferente, com a opção de incluir drivers adicionais.

1.4.3.2.6.5. Suportar a proteção de equipamentos com Microsoft Windows, suportando inclusive o backup e a recuperação do "system state" do Windows de forma nativa e sem a utilização de software de terceiros.

1.4.3.2.6.6. Suportar a criação de caches locais para o backup de notebooks com Microsoft Windows durante a ausência de conectividade de rede com a estrutura de backup, permitindo realizar os backups conforme as rotinas de backup definidas para essa área, realizando a cópia automática desses dados ao reestabelecer a conectividade.

1.4.3.2.6.7. Permitir a exclusão de diretórios e arquivos do backup.

1.4.3.2.6.8. Permitir proteger automaticamente as unidades de armazenamento externas, tal como pen drives ou HDs externos conectados, durante as rotinas de backup.

1.4.3.2.6.9. Suportar as cópias de segurança de máquinas virtuais sem a necessidade de instalação de agente.

1.4.3.2.6.10. Permitir a identificação de aplicações Microsoft Active Directory, Exchange, SQL Server

e SharePoint que residem nas máquinas virtuais, permitindo cópias de segurança consistente dessas aplicações, sem a necessidade de criação de múltiplas rotinas de backup, uma para as máquinas virtuais, e outra para as aplicações;

1.4.3.2.6.11. Permitir a integração nativa com o Microsoft Exchange on-premises (local).

1.4.3.2.6.12. Suportar a arquitetura DAG (Database Availability Group) do Exchange.

1.4.3.2.6.13. Permitir a restauração granular a nível de mensagem direto na caixa de correio do usuário.

1.4.3.2.6.14. Permitir a recuperação da mensagem em um momento do tempo específico.

1.4.3.2.6.15. Gerar logs com as informações: o que foi restaurado, quem restaurou e para onde foi restaurado.

1.4.3.2.6.16. Permitir a integração com o Microsoft SQL Server.

1.4.3.2.6.17. Executar backup de bases de dados do SQL Server de forma “online”, ou seja, sem a parada do banco.

1.4.3.2.6.18. Executar backup de logs transacionais, possibilitando a criação de rotina de backup para que ocorra em intervalos mínimos de 1 (uma) hora.

1.4.3.2.6.19. Permitir a montagem de uma base de dados SQL Server a partir dos arquivos de backup, sem necessidade de restauração completa da base para produção, permitindo executar procedimentos e visualizar dados através do SQL Server Management Studio.

1.4.3.2.6.20. Permitir recuperação granular de objetos de databases do SQL Server para o local original, ou para um servidor alternativo.

1.4.3.2.6.21. Permitir recuperação de databases para o local original ou para um servidor alternativo.

1.4.3.2.6.22. Permitir a integração com Microsoft Active Directory.

1.4.3.2.6.23. Permitir a restauração granular a nível de objeto, por exemplo, objetos de usuário incluindo suas senhas.

1.4.3.2.6.24. Permitir comparar os objetos com a produção, permitindo restaurar apenas os itens ausentes ou alterados.

1.4.3.2.6.25. Permitir a integração com Microsoft Windows File Server Failover Cluster 2016 e versões superiores.

1.4.3.2.6.26. Permitir a cópia de arquivos abertos, garantindo a consistência deles.

1.4.3.2.6.27. Permitir a integração com Oracle Database, realizando o backup de forma "online" via Oracle RMAN.

1.4.3.2.6.28. Permitir exportar uma base de dados Oracle diretamente a partir do arquivo de backup.

1.4.3.2.6.29. Permitir integração com PostgreSQL, executando o backup de bases de dados do PostgreSQL de forma “online”, ou seja, sem a parada do banco e de forma consistente.

1.4.3.2.6.30. Permitir integração com MySQL, executando o backup de bases de dados do MySQL de forma “online”, ou seja, sem a parada do banco e de forma consistente.

1.4.3.2.6.31. Deve integrar-se à tecnologia VSS (Volume Shadow Copy Service) do Windows para realizar cópias e assegurar a consistência de qualquer aplicação que disponha de um VSS Writer em estado funcional, quando da execução das cópias de segurança.

1.4.3.2.7. PLATAFORMAS DE VIRTUALIZAÇÃO

1.4.3.2.7.1. Permitir a restauração granular a nível de arquivos das máquinas virtuais protegidas, sem a necessidade de se restaurar a máquina virtual inteira.

1.4.3.2.7.2. Permitir a restauração das cópias de segurança de Máquinas Virtuais, criadas no ambiente on-premises, diretamente para instâncias AWS EC2 ou Microsoft Azure.

1.4.3.2.7.3. Permitir adicionar automaticamente as máquinas virtuais com VMware vSphere ou Microsoft Hyper-V e Nutanix AHV descobertas em rotinas de backup, com capacidade de realizar filtros avançados com critérios que incluam pelo menos datastores, clusters, resource pools, hosts, VM Folders, tags e vApps.

1.4.3.2.7.4. Permitir a recuperação de máquinas virtuais e servidores físicos instantaneamente em ambiente virtual VMware vSphere, Microsoft Hyper-V e Nutanix Acropolis, com inicialização rápida, a partir de seus arquivos de backup, sem a necessidade de esperar o término do processo de restauração.

1.4.3.2.7.5. Permitir a integração com ambiente virtual VMWare VCenter Server Appliance 8 ou superiores e deverá executar backup/recovery com as seguintes características:

1.4.3.2.7.6. Permitir a conexão com o vCenter e a exploração (descoberta) automática das máquinas virtuais.

1.4.3.2.7.7. Realizar o backup/recovery de Máquinas Virtual sem a necessidade de instalação de agente.

1.4.3.2.7.8. Realizar o armazenamento de backup das Máquinas Virtuais de maneira desduplicada.

1.4.3.2.7.9. Ser compatível com a funcionalidade VMWare VSphere CBT (Changed Block Tracking), ou seja, em vez de verificar todo o arquivo VMFS (Virtual Machine File System) deverá consultar a API (Application Programming Interface) do VMware para descobrir somente os blocos que foram alterados desde o último backup.

1.4.3.2.7.10. Permitir a inclusão automática de máquinas virtuais sem backup em seleções de backup anteriores.

1.4.3.2.7.11. Realizar a restauração da imagem completa da Máquina Virtual dentro do VMware.

1.4.3.2.7.12. Permitir redirecionar a restauração de uma da Máquina Virtual para uma pasta, datastore, hospedeiro ou rede alternativos.

1.4.3.2.7.13. Ser capaz e iniciar a execução da Máquina Virtual diretamente a partir do seu arquivo de backup, sem a necessidade de esperar o término do processo de restauração. Não serão aceitas soluções que dependam de equipamentos específicos para fornecer a tecnologia.

1.4.3.2.7.14. Realizar a restauração granular a nível de arquivos dentro sistema operacional cliente, sem a necessidade de se restaurar a Máquina Virtual inteira.

1.4.3.2.7.15. Permitir a conexão com o hospedeiro Microsoft Windows Hyper-V para a execução das rotinas de backup e restauração de dados.

1.4.3.2.7.16. Permitir a criação de rotinas de backup, rotinas de replicação e a proteção integral de aplicações hospedadas na plataforma, como Microsoft Exchange, Microsoft ShaerPoint, Microsoft SQL Server e Oracle.

1.4.3.2.7.17. Permitir a conexão com o hospedeiro Nutanix AHV e a exploração (descoberta) automática das máquinas virtuais.

1.4.3.2.7.18. Permitir a integração com ambiente virtual Nutanix AHV, identificando os domínios de proteção criados pelo Prism, e utilizando como objetos a serem protegidos pela ferramenta

de backup.

1.4.3.2.7.19. Permitir adicionar automaticamente as máquinas virtuais descobertas em rotinas de backup predefinidas, baseado no domínio de proteção que estão contidas.

1.4.3.2.7.20. Permitir adicionar automaticamente as máquinas virtuais que não foram incluídas em domínios de proteção a um grupo padrão, de forma a evitar que essas máquinas fiquem sem proteção após a sua criação.

1.4.3.2.7.21. Realizar a restauração da imagem completa da máquina virtual dentro do Nutanix AHV.

1.4.3.2.7.22. Permitir redirecionar a restauração de uma da máquina virtual para um cluster, storage container ou rede alternativos.

1.4.3.2.7.23. Permitir a recuperação de máquinas virtuais do Nutanix AHV instantaneamente no ambiente virtual, com inicialização rápida, a partir de seus arquivos de backup, sem a necessidade de esperar o término do processo de restauração.

1.4.3.2.7.24. Permitir a recuperação de um servidor físico diretamente no ambiente virtual Nutanix AHV.

1.4.3.2.7.25. Ser compatível com a funcionalidade AHV CBT (Acropolis Changed Block Tracking), para descobrir somente os blocos que foram alterados desde a última cópia de segurança.

1.4.3.2.7.26. Suportar o uso das APIs do Acropolis para backup, como o Nutanix REST API.

1.4.3.2.7.27. Permitir orquestração de Snapshots de máquinas virtuais ou Domínios de Proteção no Nutanix AHV, mantendo os dados armazenados diretamente no cluster AHV.

1.4.3.2.7.28. Permitir exportar os discos de uma máquina virtual do Nutanix AHV, a partir dos arquivos de backup, para os formatos VMDK e VHDX.

1.4.3.2.8. POLÍTICAS DE BACKUP

1.4.3.2.8.1. Suportar os métodos de backup: Full e Incremental.

1.4.3.2.8.2. Possuir no método Incremental suporte ao modo Incremental para Sempre, ou seja, as cópias de segurança devem consistir em apenas de um backup Full e todos os demais incrementais até o término do período de retenção.

1.4.3.2.8.3. Possuir no método Incremental suporte ao modo Sintético, que se assemelha ao backup incremental tradicional, todavia, ao término da cadeia de backups incrementais, o software

é capaz de sintetizar novos backups incrementais em uma imagem completa, consolidando os demais backups anteriores em uma imagem completa (full) sintética.

1.4.3.2.8.4. Permitir a geração de cópias de longa retenção full, tanto no modo ativo - executando uma nova cópia de segurança Full no cliente - quanto no modo sintético - utilizando os backups já salvos anteriormente.

1.4.3.2.8.5. Permitir o agendamento para geração automática destas cópias.

1.4.3.2.8.6. Permitir a criação de cópias secundárias ou auxiliares das imagens de backup já criadas.

1.4.3.2.9. SEGURANÇA DA INFORMAÇÃO

1.4.3.2.9.1. A solução deverá implementar mecanismos para a autenticação de usuários através de múltiplos fatores.

1.4.3.2.9.2. Deverá permitir a integração com geradores de senhas OTP (one-time password), facilitando a verificação de segunda etapa.

1.4.3.2.9.3. A solução deverá permitir habilitar, desabilitar e resetar a autenticação de duplo fator por usuário;

1.4.3.2.9.4. Possuir nativamente ferramenta que válida a implementação segura da plataforma, através da execução de testes de conformidade como:

1.4.3.2.9.5. Validação do serviço de acesso remoto (Remote Desktop);

1.4.3.2.9.6. Validação do serviço RemoteRegistry em sistemas Windows;

1.4.3.2.9.7. Validação do firewall de Windows;

1.4.3.2.9.8. Validação da versão SSL em uso na solução;

1.4.3.2.9.9. Validação do uso do protocolo SMB v1;

1.4.3.2.9.10. Validação da técnica de prevenção de perda de senhas;
1.4.3.2.9.11. A solução deverá permitir habilitar e desabilitar quais parâmetros deve ser analisado pela ferramenta de validação de conformidade.
1.4.3.2.9.12. Possuir criptografia de dados na origem (direto no cliente ou servidor de proxy de backup), de uma forma que seja garantido que o dado trafegará criptografado na LAN (Local Area Network) ou WAN (Wide Area Network).
1.4.3.2.9.13. Possuir módulo nativo de criptografia AES (Advanced Encryption Standard) 256 bits.
1.4.3.2.9.14. A solução deverá implementar diferentes chaves de criptografia por contexto de execução e proteção da plataforma de backup, com o intuito de fornecer a máxima segurança de acesso a solução, como:
1.4.3.2.9.15. Chaves de sessão, de dados e de metadados;
1.4.3.2.9.16. Chaves com informações de senha de um usuário;
1.4.3.2.9.17. Chaves para a gestão da console centralizada de gerência;
1.4.3.2.9.18. Chaves para validação de identidade no servidor de backup.
1.4.3.2.9.19. Implementar pares de chaves de criptografia de 4096 bits para recuperação de desastres.
1.4.3.2.9.20. Não serão aceitas soluções que implementem as técnicas de criptografia solicitadas através do uso de outros softwares ou plataformas integradas.
1.4.3.2.9.21. A solução deverá permitir a restauração segura de imagens de backup, permitindo a criação de uma área específica, prévia a operação de recuperação, para a varredura de vírus ou malwares.
1.4.3.2.9.22. A solução deverá possuir um arquivo de configuração o qual deverá ser validado durante o processo de restauração para identificar qual software de varredura deverá ser ativado na análise de vírus ou malwares.
1.4.3.2.9.23. Deverá ser compatível, no mínimo, com fabricantes de varredura de vírus ou malwares como: Symantec, ESET e Kaspersky.
1.4.3.2.9.24. A console de gerenciamento da solução de backup deverá exibir os resultados da varredura efetuada pelo software terceiro de análise de vírus ou malwares.
1.4.3.2.9.25. Permitir a instanciação sob demanda de uma ou mais Máquinas Virtuais, ao menos para o ambiente VMware e Hyper-V, que estejam salvas em backup, em ambiente virtual de laboratório com as seguintes características:
1.4.3.2.9.26. Prover meios automáticos de garantir a consistência das cópias de segurança a nível de aplicação, ou seja, ser capaz de automatizar a restauração de uma máquina virtual e executar ações de testes previamente programadas para aquela determinada aplicação de forma a garantir que as cópias de segurança estão consistentes.
1.4.3.2.9.27. Deverá ter a capacidade de testar a consistência das cópias de segurança, emitindo relatório de auditoria para garantir a capacidade de recuperação seguintes parâmetros: sistema operacional, aplicação e máquina virtual.

1.4.3.2.10. GERENCIAMENTO

1.4.3.2.10.1. Possuir módulo de gerenciamento central com interface gráfica (ou web) e linha de comando (interface CLI) responsáveis pela administração de todas as operações de backup, configurações, gerenciamento, monitoração, criação / atualização de políticas do ambiente e rotinas associadas à proteção de dados de todos os sites.
1.4.3.2.10.2. A solução de software de backup não deve ser operada exclusivamente por linhas de comando – CLI.
1.4.3.2.10.3. Permitir a instalação do módulo de gerenciamento e da base de dados do catálogo de metadados nos sistemas operacionais: Microsoft Windows Server 2012 ou versões superiores ou Red Hat Enterprise Linux 7 ou versões superiores.
1.4.3.2.10.4. Possuir gerenciamento das operações da infraestrutura de backup em modo gráfico, que permita o monitoramento em tempo real das rotinas de backup e status dos dispositivos e clientes de todo o ambiente.
1.4.3.2.10.5. Permitir que as tarefas abaixo sejam realizadas pela interface gráfica central, sem a necessidade de scripts e sem a necessidade de acessar a interface do cliente:
1.4.3.2.10.6. Permitir a instalação e aplicação de patches/upgrades de agentes remotamente.

1.4.3.2.10.7. Permitir configurar backup de clientes de forma remota, ou seja, toda a configuração das cópias de segurança que o cliente irá executar deve ser feita na própria console central, sem a necessidade de ter que configurar localmente o cliente.
1.4.3.2.10.8. Suportar a restauração de backup de forma remota, ou seja, na console central seleciona-se a cópia de segurança, e para onde será realizada a restauração remota.
1.4.3.2.10.9. Suportar múltiplos jobs simultâneos de backup de Máquinas Virtuais.
1.4.3.2.10.10. Possuir recursos avançados de agendamento de rotinas de backup, para datas específicas, dias da semana recorrentes, dia do mês recorrente, primeiro, segundo terceiro e último dia do mês. Ser capaz de filtrar por mês e dia da semana.
1.4.3.2.10.11. Permitir o encadeamento de jobs via interface gráfica, sem utilização de scripts, que permita a uma rotina de backup sua execução apenas após o término da outra.
1.4.3.2.10.12. Possuir agendamento de rotinas de backup, sem a utilização de utilitários de agendamento de servidores, sendo controlado pelo gerenciador de backup.
1.4.3.2.10.13. Possuir integração com Microsoft Active Directory para autenticação da Console de Gerência.
1.4.3.2.10.14. Possuir mecanismo de auditoria para o controle de acesso, em operações realizadas através de interface gráfica ou web e linha de comando (interface CLI), contendo no mínimo, as seguintes informações: data e hora da operação, usuário que realizou a operação, operação realizada.
1.4.3.2.10.15. Permitir o envio automático de alertas por e-mail e SNMP (Simple Network Management Protocol) através de traps ou consultas, com o objetivo de reportar eventos ocorridos nas operações do software de backup.
1.4.3.2.10.16. A solução deve oferecer notificações sobre problemas, bem como sobre realização de backups, por meio de logs, e-mails e mensagens na console.
1.4.3.2.10.17. Localizar um arquivo para restauração pelo nome, pesquisando no catálogo da ferramenta.
1.4.3.2.10.18. Possuir a capacidade de efetuar backup para disco e fita com retenções, através de políticas pré-definidas e agendadas.
1.4.3.2.10.19. Possuir a funcionalidade de criar múltiplas cópias de backups armazenados, com a opção de recuperação dos dados através da cópia secundária se a cópia primária não estiver mais disponível.
1.4.3.2.10.20. Possuir a função de Disk Staging, visando permitir a gravação de dados em disco e, posteriormente, a cópia para outro tipo de mídia (disco e fita).
1.4.3.2.10.21. Suportar as operações de backup e restauração via rede de dados LAN.

1.4.3.2.11. RELATÓRIOS E ASSISTÊNCIA TÉCNICA

1.4.3.2.11.1. A solução deverá permitir a visualização em sua console gráfica ou geração de relatórios de backup, os quais permitam obter minimamente as seguintes informações:
1.4.3.2.11.2. Horário de início e término de uma rotina de backup;
1.4.3.2.11.3. Tempo de duração de uma rotina de backup;
1.4.3.2.11.4. Status das cópias de segurança (situação):
1.4.3.2.11.5. Relação dos objetos incluídos na rotina de backup;
1.4.3.2.11.6. Horário de início e término das cópias de segurança de cada objeto;
1.4.3.2.11.7. Tempo de duração das cópias de segurança de cada objeto;
1.4.3.2.11.8. Volume de dados na origem durante a rotina de backup;
1.4.3.2.11.9. Volume de dados com compressão e desduplicação;
1.4.3.2.11.10. Taxa de desduplicação e compressão de dados;
1.4.3.2.11.11. Suportar a geração de relatórios sobre o consumo de licenças;
1.4.3.2.11.12. Permitir a retenção dos dados históricos por período mínimo de 12 meses.
1.4.3.2.11.13. Possuir relatórios padrões e customizáveis, disponíveis sem necessidade de alteração do código-fonte, uso de scripts ou customizações não-oficiais, devendo estar disponíveis quando da implementação da solução, contendo minimamente as seguintes características:
1.4.3.2.11.14. Permitir a segregação de acesso de acordo com o perfil do usuário, para monitorar a infraestrutura conectada;

1.4.3.2.11.15. Permitir o envio automático e programado de relatórios por e-mail;
1.4.3.2.11.16. Permitir inserir logomarca personalizada nos relatórios gerados;
1.4.3.2.11.17. Permitir exportar os relatórios gerados nos formatos: Microsoft Excel, Microsoft Word e PDF;
1.4.3.2.11.18. Suportar a geração de relatórios de "charge-back" para o ambiente de backup;
1.4.3.2.11.19. Suportar a geração e envio de alarmes automaticamente relacionados à infraestrutura virtual ou da solução de backup;
1.4.3.2.11.20. Relação sobre todos os objetos enviados para fitas, com informações sobre o tipo de dado enviado, quantidade de versões de backup enviadas e em quais fitas estão localizados os dados;
1.4.3.2.11.21. Relação sobre as fitas, com informações sobre os dados contidos nelas, espaço livre e utilizado;
1.4.3.2.11.22. Relação sobre as fitas utilizados em backups de longa retenção do tipo GFS (Grandfather-Father-Son) ou similar, com informações sobre o período de retenção, quantidade de fitas em cada conjunto, as datas em que as cópias são criadas, e em quais fitas os dados estão localizados.

1.4.3.3. Documentação para avaliação:
1.4.3.3.1. Junto ao envio da proposta comercial, na sessão do pregão, a empresa licitante deverá enviar:
datasheets, manuais ou guias de administração da solução de hardware e software de backup, para fins de avaliação técnica, sob pena de desclassificação.
1.4.3.3.2. Junto ao envio da proposta comercial, na sessão do pregão, a empresa licitante deverá enviar documento comprobatório de ser parceira credenciada do fabricante da solução de hardware e software de backup, sob pena de desclassificação.

1.4.4. Solução Firewall de Próxima Geração para Segurança de Perímetro

1.4.4.1. Pré-requisitos:
1.4.4.1.1. Os produtos de hardware ofertados devem ser novos, nunca terem sido utilizados e não terem sido descontinuados, ou seja, devem constar na linha atual de comercialização e suporte do fabricante;
1.4.4.1.2. Por se tratar de solução de segurança de alta complexidade e necessidade da implantação aderente com LGDP, na apresentação da proposta comercial a proponente deverá fornecer uma declaração do fabricante do produto ofertado, em papel timbrado, específica para este certame, declarando que a proponente possui credenciamento como revenda autorizada.
1.4.4.1.3. Os produtos ofertados deverão vir acompanhados de documentação impressa ou em mídia DVD/CD ou via download, em idioma português ou inglês, contendo orientações para configuração e operação do produto fornecido.
1.4.4.1.4. O prazo de entrega dos produtos (hardware e software) deverá ser de, no máximo, 60 (sessenta) dias corridos após o recebimento da autorização de fornecimento.
1.4.4.1.5. Deverá ser apresentado, junto à proposta comercial, no mínimo 01 (um) atestado de capacidade técnica de desempenho anterior, em nome da empresa licitante, fornecido por pessoa jurídica de direito público ou privado, que comprove a experiência da empresa licitante na execução, junto à atestante, de fornecimento de Next Generation Firewall com características equivalentes e execução dos serviços exigidos. Esse(s) atestado(s) deverá(ão) conter a identificação do(s) signatário(s) e apresentar-se em papel timbrado da empresa/órgão declarante. Poderão ser solicitadas e realizadas diligências junto a essas empresas/órgãos declarantes a fim de se confirmar e esclarecer as informações atestadas.
1.4.4.1.6. Em todo o documento são apresentadas especificações técnicas mínimas dos serviços a serem ofertados constante de todos objetos. Os termos “possui”, “permite”, “suporta” e “é” implicam no fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade requisitada. O termo “ou” implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo “e” implica que a especificação técnica mínima dos serviços será atendida englobando todas as opções.

1.4.4.2. CARACTERÍSTICAS GERAIS

1.4.4.2.1. A solução deverá ser composta de hardwares e softwares licenciados, do mesmo fabricante;

1.4.4.2.2. O prazo de garantia contratual dos bens/serviços, complementar à garantia legal prevista pelo art. 26, da Lei Federal nº. 8.078, de 1990 (Código de Defesa do Consumidor - CDC), é de, no mínimo, 60 (sessenta) meses, ou pelo prazo fornecido pelo fabricante, se superior, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

1.4.4.2.3. Todas as funcionalidades que necessitam de licenciamento, devem estar licenciadas por, no mínimo, 60 (sessenta) meses.

1.4.4.2.4. A comunicação entre os firewalls e o módulo de gerência deve ser através de meio criptografado;

1.4.4.2.5. Na data da proposta, nenhum dos produtos ofertados poderá estar/ser listado no site do fabricante em listas de end-of-life, end-of-support e/ou end-of-sale;

1.4.4.2.6. Todos os componentes devem ser próprios para montagem em rack “19” e deverão ser fornecidos: kit tipo trilho para adaptação, cabos de alimentação, suportes, gavetas e braços, se necessário;

1.4.4.2.7. Os firewalls, bem como a gerência centralizada, deverão suportar monitoramento através de SNMP v2 e v3;

1.4.4.2.8. Deve ser possível suportar arquitetura de armazenamento de logs redundante, permitindo a configuração de equipamentos distintos;

1.4.**4.3. SOLUÇÃO DE SEGURANÇA DE PERÍMETRO DE PRÓXIMA GERAÇÃO:**

1.4.4.3.1. Throughput de, no mínimo, 4 (quatro) Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicações, filtro de URL, antivírus, anti-bot e prevenção de ameaças avançadas de dia zero com log habilitado;

1.4.4.3.2. Suporte a, no mínimo, 4M (quatro milhões) de conexões simultâneas;

1.4.4.3.3. Suporte a, no mínimo, 87.000 (oitenta e sete mil) novas conexões por segundo;

1.4.4.3.4. Throughput de, no mínimo, 5 (cinco) Gbps para conexões VPN;

1.4.4.3.5. Deve suportar a performance considerando as funcionalidades de Next-Generation Firewall de 7,5 (sete e meio) Gbps, com as funcionalidades de firewall, prevenção de intrusão e controle de aplicações habilitadas;

1.4.4.3.6. Suportar e estar licenciado para acesso remoto client-to-site para 1.000 (mil) usuários;

1.4.4.3.7. Througupt de no mínimo, 9 (nove) Gbps de IPS;

1.4.4.3.8. No mínimo, 04 (quatro) interfaces de rede 10Gbps SFP+;

1.4.4.3.9. No mínimo, 16 (dezesseis) interfaces de rede 10/100/1000 base-T;

1.4.4.3.10. No mínimo, 2 (duas) interfaces de rede 2.5GbE Base-T RJ-45;

1.4.4.3.11. Caso o firewall ofertado não possua interfaces 2.5GbE Base-T RJ-45, será aceita a configuração com 02 interfaces de rede SFP+ com transceivers 10GbE Base-T RJ-45

1.4.4.3.12. Possuir 1 (uma) interface do tipo console ou similar;

1.4.4.3.13. Deve suportar operar em cluster ativo-passivo ou ativo-ativo sem a necessidade de licenças adicionais;

1.4.4.3.14. Os throughputs e as interfaces solicitados para este item deverão ser comprovados

através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces;

1.4.4.3.15. Os valores de capacidade são considerados para cada equipamento, não sendo permitido a soma dos valores dos membros do cluster;

1.4.4.3.16. Todos as medições constantes no datasheet deverão ser realizadas de modo que o tráfego seja completamente inspecionado antes de ser encaminhado, para que se privilegie a segurança frente à capacidade de encaminhamento.

1.4.4.3.17. O modo de inspeção de pacotes configurado nos concentradores, para todas as medições constantes no datasheet, deve ser de tal maneira que o payload seja montado no concentrador e seu conteúdo analisado, antes de qualquer encaminhamento de pacotes para o equipamento de destino. Dessa forma, o encaminhamento deve ser feito após análise e garantia de que não existe nenhum código malicioso no payload.

1.4.4.3.18. As medições de tráfego não devem fazer uso de técnicas de "atalho de segurança", em que os pacotes são analisados apenas parcialmente, por exemplo, tendo apenas seu cabeçalho ou os primeiros bytes verificados. Este tipo de técnica, embora consiga aumentar o throughput analisado, constitui uma brecha de segurança.

1.4.4.3.19. Se as funcionalidades acima mencionadas são habilitadas por padrão no gateway, assume-se que estavam ativas durante as medições descritas em datasheet do fabricante. Neste caso, deve-se considerar apenas 60% dos números do datasheet relativos a throughput inspecionado, ou seja, multiplicá-los por um fator de 0,6.

1.4.4.3.20. Todas as interfaces fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato, incluindo seus transceivers/transceptores. Caso sejam fornecidas interfaces além das exigidas, todas as interfaces devem ser fornecidas com todos os transceivers/transceptores necessários para a plena utilização;

1.4.4.4. FUNCIONALIDADE DE FIREWALL

1.4.4.4.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;

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

1.4.4.4.3. O hardware e software que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

1.4.4.4.4. A solução de segurança deve usar Stateful Inspection com base na análise granular de comunicação e de estado do aplicativo para monitorar e controlar o fluxo de rede;

1.4.4.4.5. Realizar upgrade via SCP, SFTP e https via interface WEB

1.4.4.4.6. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

1.4.4.4.6.1. Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast, DHCP Relay, DHCP Server e Jumbo Frames;

1.4.4.4.7. Deve suportar os seguintes tipos de NAT:

1.4.4.4.7.1. NAT dinâmico (Many-to-1), NAT estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente;

1.4.4.4.8. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH,

facilitando a localização de comandos;

1.4.4.4.9. Deverá permitir a criação de regras de firewall e NAT utilizando nos campos de origem e destino, objetos de serviços online atualizavéis de forma dinâmica, por exemplo: Office 365, AWS, Azure e outros. Objetos dinâmicos que não se caracterizam como FQDN.

1.4.4.4.10. Enviar logs para sistemas de monitoração externos, simultaneamente;

1.4.4.4.11. Prover mecanismo contra-ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção;

1.4.4.4.12. Deve realizar roteamentos unicast e multicast simultaneamente em uma única instância(contexto) de firewall.

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

1.4.4.4.14. Suportar OSPF graceful restart;

4.4.15. Autenticação integrada via Kerberos.

1.4.4.4.16. Nao serao aceitas solucoes nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas;

1.4.4.4.17. A solução deve ter a capacidade de operar através de uma unica instancia de Firewall de forma simultânea mediante o uso das suas interfaces fisicas nos seguintes modos: transparente, mode sniffer (monitoramento e análise o trafego de rede), camada 2 (L2) e camada 3 (L3);

1.4.4.4.18. A solução deve permitir salvar as configurações das políticas para serem aplicadas em horarios pré-definidos;

1.4.4.4.19. Deve possuir mecanismo de ativação de validada da regra com período customizado;

1.4.4.4.20. Deverá suportar redundância e balancemento de links, tendo capacidade a no minimo 3 links de internet.

1.4.4.4.21. Deverá suportar configurar um valor de threshold baseando-se em critérios mínimos como fator de decisão nas regras de balanceamento.

1.4.4.4.22. Deve permitir a configuração do tempo de checagem para cada um dos links.

1.4.4.5. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

1.4.4.5.1. Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;

1.4.4.5.2. Controle de políticas por usuários, grupos de usuários, IPs e redes;

1.4.4.5.3. Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2 e TLS 1.3

1.4.4.5.4. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

1.4.4.5.5. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

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

1.4.4.5.5.2. Reconhecer pelo menos 6.000 (seis mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

1.4.4.5.6. A checagem de assinaturas deve determinar se uma aplicação está utilizando a porta padrão ou não;

1.4.4.5.7. Para inspeção SSL, ou HTTPS Inspection, a solução deve oferecer suporte ao Perfect Forward Secrecy (conjuntos de cifras PFS, ECDHE)

1.4.4.5.8. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;

1.4.4.5.9. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo;

1.4.4.5.10. A fim de otimização de tempo operacional dos administrdores, a solução deverá possuir pelo menos 120 categorias de aplicações WEB pré-definidas pelo fabricante;

1.4.4.5.11. Para solução de filtro de conteúdo e controle web, deve ser capaz de bloquear na mesma aplicação um conteúdo específico sem bloquear a aplicação principal (Ex.: Whatsapp Web, Whatsapp voice e Whatsapp file transfer.);

1.4.4.5.12. Possui mecanismo de controle de aplicação web e URL que possui configuração de bloqueio e liberação da aplicação princial e/ou as suas sub-categorias. Quando o administrador da solução desejar bloquear apenas as sub-categorias do facebook, como facebook chat, video, game, compartilhamento de arquivos ou outros. Ou seja, não deve ser bloqueado toda a categoria como “Facebook” ou "Redes sociais" que também pode implicar o bloqueio não só do Facebook, mas também bloqueará tudo que estiver relacionado às redes sociais, como LinkedIn, Twitter, YouTube, etc. A solução precisa ser baseada em bloqueio de applicações WEB que a propria base possui, assim a inspeção ocorrerá em camada 7 analisando o payload do pacote.

1.4.4.5.13. A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação;

1.4.4.5.14. Atualizar a base de assinaturas de aplicações automaticamente;

1.4.4.5.15. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;

1.4.4.5.16. Os dispositivos de proteção de rede devem possuir a capacidade de identificar de forma transparente o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários. Assim, permitindo a criação de politicas de segurança baseadas nas informações coletadas entre elas usuários, IP, grupos de usuários do sistema do Active Directory;

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

1.4.4.5.18. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

1.4.4.5.19. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

1.4.4.5.20. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

1.4.4.5.20.1. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

1.4.4.5.20.2. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

1.4.4.5.20.3. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs atráves da integração com serviços de

diretório, autenticação via Active Directory e base de dados local;

1.4.4.5.20.4. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

1.4.4.5.20.5. Suportar armazenamento, na própria solução, de URLs, evitando delay de comunicação/validação das URLs;

1.4.4.5.20.6. Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção “Safe Search” esteja desabilitada no navegador do usuário;

1.4.4.5.20.7. Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja solução de software livre;

1.4.4.5.20.8. Suportar a criação de categorias de URLs customizadas;

1.4.4.5.20.9. Suportar a exclusão de URLs do bloqueio, por categoria;

1.4.4.5.20.10. Permitir a customização de página de bloqueio;

1.4.4.5.21. 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, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede;

1.4.4.5.22. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius ou API’s ou Syslog, para a identificação de endereços IP e usuários;

1.4.4.5.23. Deve permitir o controle, sem instalação de cliente de software, em máquinas/computadores que solicitem saída à internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no Firewall (Captive Portal);

1.4.4.6. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS

1.4.4.6.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento de firewall;

1.4.4.6.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques prédefinidos;

1.4.4.6.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/passivo;

1.4.4.6.4. Deve suportar granularidade nas políticas de Antivírus e Anti-malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

1.4.4.6.4.1. A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo;

1.4.4.6.5. Deverá possuir os seguintes mecanismos de inspeção de IPS:

1.4.4.6.5.1. Análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

1.4.4.6.6. Detectar e bloquear a origem de portscans;

1.4.4.6.7. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

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

1.4.4.6.9. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;

1.4.4.6.10. Suportar bloqueio de arquivos por tipo;

1.4.4.6.11. Identificar e bloquear comunicação com botnets;

1.4.4.6.12. Deve suportar referência cruzada com CVE;

1.4.4.6.13. Em cada proteção de segurança, deve estar incluso informações como:

1.4.4.6.13.1. Código CVE (Common Vulnerabilities and Exposures), não sendo aceito outro codigo de referência;

1.4.4.6.13.2. Severidade;

1.4.4.6.13.3. Tipo de ação a ser executada.

1.4.4.6.14. O IPS deve fornecer um mecanismo automatizado para ativar ou gerenciar novas assinaturas vindas de atualizações.

1.4.4.6.15. O IPS deve suportar exceções de rede com base na origem, destino, serviço ou uma combinação dos três.

1.4.4.6.16. O IPS deve incluir um modo de solução de problemas que defina o perfil em uso para detectar apenas, sem modificar as proteções individuais.

1.4.4.6.17. O administrador deve poder ativar automaticamente novas proteções, com base em parâmetros configuráveis (impacto no desempenho, gravidade da ameaça, nível de confiança, proteção do cliente, proteção do servidor)

1.4.4.6.18. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

1.4.4.6.18.1. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;

1.4.4.6.19. Na própria interface de gerência, a solução de IPS deverá apresentar sumário de todos os equipamentos que estão sendo gerenciados, assim como, qual o tipo de perfil assinalado, de forma individual;

1.4.4.6.20. A solução de IPS, deve possuir mecanismo de análise baseado nas conexões realizadas para as aplicações, que aponta quais assinaturas que estão em modo detecção deve ser alterada para modo prevenção, assim evitando qualquer tipo de ataque para aplicações que estão expostas no ambiente.

1.4.4.6.21. O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados na funcionalidade de IPS;

1.4.4.6.22. A solução deverá possuir pelo menos dois perfis pré-configurados pelo fabricante que permitam sua utilização assim que o equipamento for configurado;

1.4.4.6.23. A solução deve permitir que o administrador possa configurar quais métodos e comandos HTTP são permitidos e quais são bloqueados.

1.4.4.6.24. Deve incluir proteção contra vírus em conteúdo ActiveX e applets Java e worms;

1.4.4.6.25. Solução deve proteger contra os ataques do tipo DNS Cache Poisoning, e impedir que os

usuários acessem endereços de domínios bloqueados;

1.4.4.6.26. O gerenciamento centralizado via interface gráfica, deve possibilitar a configuração de captura dos pacotes por regras individuais, visando aperfeiçoar o desempenho do equipamento;

1.4.4.6.27. A solução de IPS deve possuir engine onde irá determinar de forma automatica, onde qualquer nova assinatura que for baixada na base local deverá atuar em modo de prevenção ou detecção, assim evitará qualquer tipo de alteração na base de assinatura atual;

1.4.4.6.28. O antivírus deve oferecer suporte à verificação de links dentro de emails.

1.4.4.6.29. A solução de anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede quando usuário estiver conectado com ambiente externo malicioso

1.4.4.6.30. A solução deve permitir criar regras de exceção de acordo com a proteção, a partir do log visualizado na interface gráfica da gerência centralizada;

1.4.4.6.31. Para melhor administração a solução deve possuir a granularidade na classificação das proteções de IPS através de: severidade, nível de confiança da proteção, impacto da performance, referência de indústria terceira e status de download recente;

1.4.4.6.32. A solução deve permitir a criação de White list baseado no MD5 do arquivo;

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

1.4.4.6.34. A funcionalidade de IPS e anti-bot, deve possuir capacidade de correlacionar em seus logs a visibilidade de acordo com o framework ATT&CK Mitre Matrix, pontuando características de técnicas de acordo com a ameaça detecada/bloqueada pela solução. Caso a solução não possua determinada capacidade, poderá ser integrada com outra solução de mercado, não sendo ela soluções abertas;

1.4.4.6.35. Suportar rastreamento de vírus em arquivos pdf;

1.4.4.6.36. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);

1.4.4.6.37. Possuir a capacidade de prevenção de ameaças não conhecidas;

1.4.4.6.38. Em caso de falha no mecanismo de inspeção do Anti-Virus, deve ser possível configurar se as conexões serão permitidas ou bloqueada

1.4.4.6.39. A solução de Anti-virus e Anti-Malware deve funcionar de forma independente, ou seja, caso sejam desabilitadas, elas não podem causar a interrupção de outras funcionalidades de segurança como prevenção de ameaças avançadas (zero-day);

1.4.4.6.40. A solução Antivirus deverá suportar análise de arquivos que tráfegam dentro do protocolo CIFS/SMB, de forma a conter malwares se espalhando horizontalmente pela rede;

1.4.4.6.41. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;

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

1.4.4.6.43. A solução deverá possuir mecanismo de “machine learning” para prevenção de ataques de DNS do tipo DGA (Domain Genaration Algorith) não sendo aceito soluções que usem apenas mecanismo baseado em assinaturas.

1.4.4.6.44. A solução deverá possuir mecanismo de “machine learning” para prevenção de ataques de DNS Tunneling, não sendo aceito soluções que usem apenas mecanismo baseado em assinaturas.

1.4.4.6.45. Deverá possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos, sejam resolvidas pelo Firewall com endereços previamente

definidos, para interceptar a comunicação e bloquear o acesso do usuário.

1.4.4.6.46. A solução de Anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede.

1.4.4.6.47. A solução deve possuir funcionalidade de identificação de bloqueio de trafego malicioso comunicando com C&C (command & Control);

1.4.4.6.48. A solução Antivirus deverá suportar a análise de links no corpo de emails.

1.4.4.7. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO

1.4.4.7.1. Suportar a criação de políticas de QoS por:

1.4.4.7.2. Endereço de origem, endereço de destino e por porta;

1.4.4.7.3. O QoS deve possibilitar a definição de classes por:

1.4.4.7.4. Banda garantida, banda máxima e fila de prioridade;

1.4.4.7.5. Disponibilizar estatísticas em tempo real para classes de QoS;

1.4.4.8. FUNCIONALIDADES DE VPN

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

1.4.4.8.2. Suportar IPSec VPN;

1.4.4.8.3. A solução deve suportar Autoridade Certificadora Interna e Externa (de terceiros);

1.4.4.8.4. Suportar SSL VPN;

1.4.4.8.5. A VPN IPSEc deve suportar:

1.4.4.8.5.1. 3DES, Autenticação MD5, SHA-1, SHA-384, AES-XCBC, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard), SHA-512 e Autenticação via certificado IKE PKI;

1.4.4.8.6. A VPN SSL deve suportar:

1.4.4.8.6.1. Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento;

1.4.4.8.6.2. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

1.4.4.8.6.3. Suportar configuração de comformidade para acesso do usuário via portal SSL ou cliente na maquina do usuário;

1.4.4.8.6.4. Atribuição de endereço IP nos clientes remotos de VPN;

1.4.4.8.6.5. Atribuição de DNS nos clientes remotos de VPN;

1.4.4.8.6.6. Dever permitir criar políticas para tráfego dos clientes remotos conectados na VPN SSL;

1.4.4.8.6.7. Suportar autenticação via AD/LDAP, certificado e base de usuários local;

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

1.4.4.8.6.9. A tecnologia de VPN Client to Server deverá ser instalada na plataforma: iOS 10 ou superior e Android;

1.4.4.8.6.10. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows 7, Windows 8 e MacOS X;

1.4.4.9. SOLUÇÃO PARA PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS – ZERO DAY

1.4.4.9.1. A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT;

1.4.4.9.2. A solução deverá ser composta por hardware e software específicos (appliance) com sistema operacional especializado em sua versão mais atualizada ou nuvem do proprio fabricante que possui o conceito de sandboxing para prevenção de ataques zero-day.

1.4.4.9.3. Não será aceito soluções que dependa da estrutura de hypervisor do contratante para a análise de ameaças de dia zero, como Vmware ESXi, Microsoft HyperV, entre outros;

1.4.4.9.4. Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS), FTP e durante análise completa do arquivo no ambiente sandbox, sem que o mesmo seja entregue parcialmente ao cliente.

1.4.4.9.5. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;

1.4.4.9.6. A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows XP, Windows 7, Windows 8.1 e Windows 10, assim como Office 2003, 2010, 2013 e 2016;

1.4.4.9.7. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas antes de entregar este arquivo para o cliente;

1.4.4.9.8. O conteúdo enviado para a solução de Sandboxing deverá ser feito automaticamente, sem a necessidade da interação do usuário/administrador para que o processo de análise seja realizado;

1.4.4.9.9. Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, dias da semana ou dias do mês assim como o período de cada atualização;

1.4.4.9.10. Toda análise dos arquivos deverá ser realizada em ambiente controlado Sandboxing em nuvem. Não serão aceitas soluções em servidores ou software livre;

1.4.4.9.11. A funcionalidade de prevenção de ameaças avançadas deve ser habilitada e funcionar de forma independente das outras funcionalidades de segurança;

1.4.4.9.12. Toda análise deverá ser realizada em nuvem do próprio fabricante, não sendo aceitas soluções que necessitem de módulos e/ou servidores externos para a implementação de máquinas virtuais;

1.4.4.9.13. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF acima de 10 Mb;

1.4.4.9.14. Deve implementar análise em sandbox, detecção e bloqueio de malwares em arquivos executáveis, DLLs, ZIP e criptografados em SSL;

1.4.4.9.15. Deve implementar análise em sandbox, detecção e bloqueio de malwares em arquivos java
(.jar e class);

1.4.4.9.16. A solução deve suportar inspeção para o protocolo SMBv3;

1.4.4.9.17. O relatório das emulações deve conter print screen dos arquivos emulados, assim como todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado;

1.4.4.9.18. A solução deve possuir engine de inspeção a nivel de CPU para detectar técnicas ROP (Return Of Operation) além de outras técnicas de exploração de vulnerabilidade monitorando o

fluxo de CPU;

1.4.4.9.19. Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;

1.4.4.9.20. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;

1.4.4.9.21. Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, seven-z, exe rtf, csv, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, doc, docx, dot, docm, dotx, dotm e gz;

1.4.4.9.22. Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real e o bloqueio deve ser imediato, não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;

1.4.4.9.23. Possibilitar remoção de conteúdo ativo dinâmicos como macros, URL's, Java scripts e outros dos arquivos baixados, permitindo o download do arquivo original caso ele não seja malicioso;

1.4.4.9.24. A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;

1.4.4.9.25. A solução deve possuir mecanismo de inteligência artificial para identificar e prevenir sites conhecidos e desconhecidos como phishing, analisando em tempo real a URL acessada.

1.4.4.9.26. Caso seja identificado como um site de phishing a solução deverá bloquear o acesso do usuário ao tentar fazer o envio de suas credenciais.

1.4.4.9.27. O mecanismo de classificação anti-phising deve atuar sem a necessidade de instalação de agente na máquina do usuário;

1.4.4.9.28. Para melhor administração da solução, a solução deve possibilitar as seguintes 1.4.visualizações a nível de monitoração:

1.4.4.9.28.1. Número de arquivos emulados;

1.4.4.9.28.2. Número de arquivos com malware.

1.4.4.9.29. A solução de prevenção de ameaças avançada, deve possuir capacidade de apresentar em seus logs, visibilidade de acordo com o framework ATT&CK Mitre Matrix, pontuando características de táticas e técnicas de acordo com a ameaça detecada/bloqueada pela solução. Caso a solução não possua determinada capacidade, poderá ser integrada com outra solução de mercado, não sendo ela soluções abertas;

1.4.4.9.30. A solução deve prover informação, seja por meio de relatório ou log, sobre as seguintes situações:

1.4.4.9.30.1. O tamanho máximo do arquivo emulado seja excedido;

1.4.4.9.30.2. O tempo máximo de emulação seja excedido.

1.4.4.10. SOLUÇÃO DE GERENCIAMENTO E RELATÓRIOS

1.4.4.10.1. A solução de gerência deverá ser separada dos gateways de segurança, que irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas neste documento;

1.4.4.10.2. Caso a solução possua licenças relacionadas a capacidade de log indexados e armazenamento, deve ser ofertado com indexação de, no mínimo, 200 GB/dia ou ilimitada;

1.4.4.10.3. Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução;

1.4.4.10.4. Deve possuir solução de gerenciamento e administração centralizado, possibilitando o gerenciamento de diversos equipamentos de proteção de rede do mesmo fabricante desde que não sejam software livre;

1.4.4.10.5. O módulo de gerência deve ser capaz de gerenciar e administrar todas as soluções descritas neste termo;

1.4.4.10.6. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;

1.4.4.10.7. Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento;

1.4.4.10.8. O gerenciamento da solução deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS);

1.4.4.10.9. Todos os logs da solução devem ser indexados e seu licenciamento deve ser o de maior capacidade.

1.4.4.10.10. O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores;

1.4.4.10.11. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

1.4.4.10.12. Suportar criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração;

1.4.4.10.13. Suportar backup das configurações e rollback de configuração para a última configuração salva;

1.4.4.10.14. Suportar validação de regras antes da aplicação;

1.4.4.10.15. Suportar validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

1.4.4.10.16. Deve permitir a visualização dos logs de uma regra específica em tempo real e na mesma tela de configuração da regra selecionada;

1.4.4.10.17. Deve possibilitar a integração com outras soluções de SIEM de mercado desde que não sejam software livre;

1.4.4.10.18. Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

1.4.4.10.19. Permitir a criação de certificados digitais para autenticação de usuários;

1.4.4.10.20. O relatório deve apresentar eventos em um unico portal (dashboard) e geração de relatório de todas as funcionalidades de segurança que estão ativadas nos GW’s de segurança, sendo que deve possuir relatório e telas de apresentação onde consta todo os principais eventos das funcionalidades de controle de aplicação web, filtro URL, prevenção de ameaças (IPS, Antivírus, Anti-Malware e Sandboxing);

1.4.4.10.21. A solução deve permitir o login de multiplos usuários administradores simultaneos com perfil de escrita, possibilitando agilidade e rapidez no gerenciamento pelo grupo de administradores da solução.

1.4.4.10.22. A solução deve permitir a integração da ferramenta com provedores de identidade para authenticação dos administradores da solução via SAML 2.0;

1.4.4.10.23. A solução deve permitir revisar e aprovar alterações de políticas de segurança feitas por outros administradores.

1.4.4.10.24. A solução deve permitir criar perfis de administradores para realizar revisão/alteração das políticas de segurança, com no minimo, os perfis de aprovador e solicitante.

1.4.4.10.25. A solução deverá enviar a solicitação de aprovação de políticas de segurança por pelo menos uma das seguintes formas, Email, Requisição WEB ou Scripts.

1.4.4.10.26. A solução deve possuir logs, correlação de eventos e relatórios de auditoria dos administradores da solução;

1.4.4.10.27. Permitir criação de relatórios customizados via interface gráfica, sem necessidade de conhecer linguagens de banco de dados;

1.4.4.10.28. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, AntiMalware), e URLs que passaram pela solução;

1.4.4.10.29. Deve ser possível exportar os logs em CSV ou TXT;

1.4.4.10.30. A solução deve ser capaz de segmentar a base de regras em uma estrutura em camadas;

1.4.4.10.31. A solução deve ser capaz de aplicar proteções relacionadas a ameaças e regras de acesso separadamente;

1.4.4.10.32. A solução deve combinar configuração de políticas e análise de logs em um único painel, para evitar erros alcançando maior confiabilidade na alteração de políticas;

1.4.4.10.33. O visualizador de log deve ter um recurso de pesquisa de texto livre;

1.4.4.10.34. Deve possibilitar a geração de relatórios de eventos no formato PDF ou HTML;

1.4.4.10.35. Possibilitar rotação do log;

1.4.4.10.36. Suportar geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

1.4.4.10.37. Resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda, principais aplicações por taxa de transferência de bytes, principais hosts por número de ameaças identificadas, atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Malware), de rede vinculadas a este tráfego;

1.4.4.10.38. Deve permitir a criação de relatórios personalizados;

1.4.4.10.39. O gerenciamento centralizado deverá ser entregue como appliance virtual e dever ser compatível/homologado com/para VMWare ESX (vSphere 5.1, 5.5 ou 6;

1.4.4.10.40. A solução de gerenciamento deve possuir a capacidade de gerenciar outros Firewalls de segurança do mesmo fabricante mesmo estando em ambientes virtualizados e nuvens publicas (AWS e Azure) e nuvens privadas (VmWare NSX ou Cisco ACI);

1.4.4.10.41. Possiu capacidade de integração com soluções de terceiros via API e também suportar configurações através de RestAPI.

1.4.4.10.42. A solução deverá ser capaz de automatizar a contenção de ataques, impedindo que eles se espalhem pela rede através da execução de ações preventivas coordenadas e imediatas.

1.4.4.10.43. A solução deverá alertar automaticamente as equipes de segurança assim que uma ameaça for detectada, minimizando o tempo de resposta e permitindo ações corretivas rápidas e eficazes.

1.4.4.10.44. A solução deverá ser capaz de integrar-se com sistemas de gerenciamento de fluxo de

trabalho existentes, como pelo menos os seguintes serviços, ServiceNow, Jira e Microsoft Teams, para facilitar a coordenação e o gerenciamento de respostas a incidentes.

1.4.4.10.45. A solução deverá fornecer a capacidade personalizar playbooks de automação, permitindo que as organizações ajustem as respostas automáticas.

1.4.4.10.46. O modulo de automação deverá permitir pelos menos as seguintes automações:

1.4.4.10.46.1. Bloquear ataques de scanners identificados pelo IPS;

1.4.4.10.46.2. Notificar quando um super usuários fizer login via CLI nos equipamentos;

1.4.4.10.46.3. Notificar quando for executar script quando;

1.4.4.10.46.4. Quarentenar endereços IPs;

1.4.4.10.47. Deve consolidar logs e relatórios de todos os dispositivos administrados;

1.4.4.10.48. Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;

1.4.4.10.49. Deverá possuir mecanismo de Drill-Down para navegação e análise dos logs em tempo real;

1.4.4.10.50. Nas opções de Drill-Down, deve ser possível identificar o usuário que fez determinado acesso;

1.4.4.10.51. Permitir que os relatórios possam ser salvos, enviados e impressos;

1.4.4.10.52. Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino, etc;

1.4.4.10.53. A solução deve prover, no mínimo, as seguintes funcionalidades para análise avançada dos incidentes:

1.4.4.10.53.1. Visualizar quantidade de tráfego utilizado de aplicações e navegação;

1.4.4.10.53.2. Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;

1.4.4.10.54. A solução de correlação deve possuir mecanismo para detectar login de administradores em horários irregulares;

1.4.4.10.55. A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

1.4.4.10.56. Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando para tantos gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos;

1.4.4.10.57. Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory via Radius;

1.4.4.10.58. Criar certificados digitais para acesso dos usuários VPN;

1.4.4.10.59. Criar certificados digitais para VPNs Site-to-Site;

1.4.4.10.60. Caso a solução possua licenciamento relacionado a capacidade de criação de certificados, deve ser contemplado para no mínimo 1000 certificados ou ilimitada;

1.4.4.10.61. Permitir criações de políticas de acesso de usuários autenticada no Active Directory, de forma que reconheça os usuários de forma transparente;

1.4.4.10.62. Geração de painel e relatórios contendo mapas geográficos gerados em tempo real para a visualização das principais ameaças através de origens e destinos do tráfego gerado na Instituição.

1.4.4.10.63. A plataforma de gerência centralizada e monitoração deve possibilitar a visualização dos logs de Firewall, navegação web, conteudo de arquivos, prevenção de ameaças e Sandbox, todos a partir de um único local centralizado possibilitando a procura correlacionada de logs em uma única tela, como por exemplo pesquisar logs de Antivirus e navegação web simultaneamente na mesma query de pesquisa.

1.4.4.10.64. O relatório das emulações (sandboxing) deve conter print screen dos arquivos emulados, assim como todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado;

1.4.4.10.65. A plataforma de gerência centralizada e monitoração deve possibilitar a procura por IPs e redes, sendo que os resultados mostrem estes Pps e redes nos campos de origem e destino dos logs na mesma tela de pesquisa.

1.4.4.10.66. Possuir mecanismo para que logs antigos sejam removidos automaticamente;

1.4.4.10.67. Possuir a capacidade de personalização de gráficos como barra, linha e tabela;

1.4.4.10.68. Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;

1.4.4.10.69. Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU;

1.4.4.10.70. A solução deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real;

1.4.4.10.71. A solução deve fornecer conteúdo de correlação pré-definido organizado por categoria;

1.4.4.10.72. A solução deve ser capaz de personalizar e criar regras de correlação;

1.4.4.10.73. A solução deve fornecer uma interface gráfica para criação das regras citadas no item anterior;

1.4.4.10.74. A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências;

1.4.4.11. Documentação para avaliação:

1.4.4.11.1. Junto ao envio da proposta comercial, na sessão do pregão, a empresa licitante deverá enviar: datasheets, manuais ou guias de administração da solução de firewall, para fins de avaliação técnica, sob pena de desclassificação.

1.4.4.11.2. Junto ao envio da proposta comercial, na sessão do pregão, a empresa licitante deverá enviar documento comprobatório de ser parceira credenciada do fabricante da solução de firewall, sob pena de desclassificação.

1.4.5. Solução de Segurança para Datacenter

1.4.5.1. Características Gerais

1.4.5.1.1. Não serão aceitos produtos ou serviços do tipo demo, trial e open-source. A solução deve ser proprietária.

1.4.5.1.2. A solução de Segurança de Datacenter deverá ser fornecida em appliance virtual.

1.4.5.1.3. O appliance virtual deverá ser compatível para operar em VMWARE, KVM e NUTANIX,

além de estar disponível no marketplace da AWS, GCP e Azure para contratação no modelo Bring Your Own License (BYOL).

1.4.5.1.4. A solução deve ser capaz de visualizar, via console, as informações de saúde e desempenho de todo o ambiente que a compõem, incluído softwares e equipamentos.

1.4.5.1.5. Possuir suporte a SNMP v2c e v3.

1.4.5.1.6. Enviar mensagens por e-mail e traps SNMP.

1.4.5.1.7. Os componentes da solução poderão ser executados num mesmo appliance, ou poderão ser distribuídos em múltiplos appliances, de acordo com a característica de cada produto, respeitadas as características de funcionamento e performance exigidas neste edital.

1.4.5.1.8. A solução deverá ter o pleno funcionamento independentemente de conexão (física ou lógica) com o fabricante, exceto para atualizações de versões e de segurança.

1.4.5.1.9. Suportar IPV6.

1.4.5.1.10. A solução deverá possuir a capacidade para suportar a adição de novos componentes (hardware e/ou software) escaláveis sem causar interrupções no funcionamento da solução.

1.4.5.1.11. Apresentar uma relação descritiva dos componentes fornecidos, incluindo seus códigos comerciais.

1.4.5.1.12. Não será aceito equipamento do tipo NGFW (Next Generation Firewall).

1.4.5.2. **Características do Appliance**

1.4.5.2.1. Deve ser capaz de executar todas as suas funções de aprendizado, análise e proteção de tráfego web considerando pelo menos uma taxa de transferência de 200 Mbps.

1.4.5.2.2. A solução deve ter vários mecanismos de implantação (deployment) com pelo menos uma ponte transparente na linha (Bridge L2), Proxy Reverso. Deve possuir a capacidade de monitorar e auditar todos os acessos de modo (passivo) a fim de monitorar o tráfego sem fazer alterações na rede.

1.4.5.2.3. A solução deve permitir a integração nos modos proxy reverso explícito e proxy reverso transparente (Bridge L2).

1.4.5.2.4. A solução deve ter um impacto de milissegundos na latência da rede.

1.4.5.2.5. O sistema deve permitir a integração e envio de alertas para terceiros ou ferramentas de correlação (SIEM). Será permitido que a integração seja realizada através da exportação de eventos utilizando SYSLOG ou através de RestAPI.

1.4.5.2.6. O appliance deve suportar o protocolo de gerenciamento de rede SNMP a ser monitorado por ferramentas de terceiros.

1.4.5.2.7. Todos os componentes da solução ADC deve estar com recursos para efetuar o balanceamento de carga entre aplicações e devem ser de um mesmo fabricante, ou serem homologados pelo mesmo, ou compatíveis com outros fabricantes, podendo a CONTRATANTE realizar diligência junto ao mesmo para esta comprovação quando da recepção técnica da solução. As funcionalidades de WAF e balanceamento de carga entre aplicações web deve ser ofertadas no mesmo appliance;

1.4.5.2.8. A solução ADC com balanceamento de carga entre aplicações web e WAF ofertada deve operar de forma integrada e deve ser composta de no mínimo um cluster com dois applicances.

1.4.5.2.9. Caso a solução de WAF seja ofertada separadamente da solução balanceamento de carga entre aplicações Web, tanto a solução de WAF quanto a solução de balanceamento deve ser composta de no mínimo um cluster com dois applicances ou servidores cada.

1.4.5.2.10. A solução de WAF e a solução de balanceamento entre aplicações web devem ser do mesmo fabricante.

1.4.5.2.11. A capacidade de processamento da solução deverá seguir as melhores práticas de cada fabricante, considerando todos os requisitos de capacidade definidos nesta especificação, tais como: trafego, conectividade, conexões, requisições nível 7, requisições SSL, transações e compressão.

1.4.5.2.12. Deve possui CPU e memoria suficientes para atender os throughputs definidos no edital tanto para WAF quanto para o balanceador sem degradação de performance da solução quando ativada simultaneamente as duas funcionalidades.

1.4.5.2.13. Os equipamentos que serão responsáveis pela inspeção de tráfego web e pelo balanceamento de carga para soluções ofertadas em appliances distintos, deverão suportar, cada um de forma independente, o throughput de pelo menos 200 (DUZENTOS) Mbps tanto para a funcionalidade de firewall de aplicação Web como para a funcionalidade de balanceamento de carga entre aplicações.

1.4.5.2.14. As soluções de WAF com balanceamento ofertadas no mesmo appliance deverão suportar o throughput de pelo menos 200 (DUZENTOS) Mbps em cada appliance do cluster.

1.4.5.2.15. Suportar IPv4 e IPv6;

1.4.5.2.16. Suportar múltiplas tabelas de roteamento independentes em IPv4 e IPv6;

1.4.5.2.17. Suportar VXLAN para integração com o ambiente de virtualização;

1.4.5.2.18. Suportar configuração de endereçamento IP estático e dinâmico (DHCP/BOOTP) para o gerenciamento;

1.4.5.2.19. Suportar implementação em alta disponibilidade:

1.4.5.2.19.1. Implementar modo ativo/standby;

1.4.5.2.19.2. Suportar modo ativo/ativo para, pelo menos, as funções de balanceamento de servidores. Aceita-se como ativo/ativo a utilização de dois endereços virtuais, onde cada endereço fica ativo em um elemento e standby no outro;

1.4.5.2.19.3. Permitir a sincronização das configurações de forma automática e manual, forçando a sincronização quando necessário;

1.4.5.2.19.4. Permitir utilizar qualquer endereçamento IP, inclusive os definidos na RFC 1918, para criação de cluster, hearbeat e sincronização entre os equipamentos;

1.4.5.2.19.5. Fornecer todos os recursos de redundância da solução sem nenhuma despesa com licenças adicionais;

1.4.5.2.19.6. Permitir expansão do cluster adicionando novos equipamentos inclusive de modelos diferentes;

1.4.5.3. **Balanceamento, Cache e Aceleração Web**

1.4.5.3.1. Deve suportar no mínimo 200 Mbps (DUZENTOS) de inspeção de tráfego na camada 7. Para alcançar esse throughput será aceito que o equipamento faça cache, em memória RAM ou SSD, do conteúdo estático, como por exemplo imagens, após a sua primeira inspeção. Todo conteúdo estático permitido em cache não será reinspecionado até a expiração do cache.

1.4.5.3.2. A solução fornecida deverá operar em cluster oferecendo alta disponibilidade com tolerância a falhas, independentemente da quantidade de elementos que compõe o cluster.

1.4.5.3.3. Na falha de um dos elementos do cluster, não poderá haver nenhuma degradação ou indisponibilidade das aplicações.

1.4.5.3.4. Possuir interface gráfica via web e interface via CLI por SSH e console para administração, gerenciamento e monitoramento do equipamento;

1.4.5.3.5. Implementar o SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol);

1.4.5.3.6. Permitir habilitar e desabilitar acesso administrativo via SSH por qualquer interface do equipamento;

1.4.5.3.7. Manter internamente múltiplos arquivos de configurações do sistema;

1.4.5.3.8. Utilizar SCP ou HTTPS como mecanismo de transferência de arquivos de configuração e sistema operacional;

1.4.5.3.9. Possuir recurso de autocompletar nos comandos na CLI, com ajuda contextual;

1.4.5.3.10. Permitir a configuração de múltiplas contas locais de administradores;

1.4.5.3.11. Implementar controles de acesso por nível, os quais podem ser atribuídos a usuários ou grupos de usuários para fazer cumprir a separação por perfil de privilégios;

1.4.5.3.12. Possuir, no mínimo, três níveis de usuários na GUI: administrador, analista e somente-leitura;

1.4.5.3.13. Suportar autenticação e autorização externa de usuários administradores através de RADIUS, LDAP, Active Directory e TACACS+;

1.4.5.3.14. A interface gráfica deve permitir a atualização do sistema operacional, atualização de componentes e instalação de patches;

1.4.5.3.15. Permitir selecionar pela interface gráfica a versão do sistema operacional para inicialização do equipamento;

1.4.5.3.16. Possuir um comando, via CLI, que mostre o tráfego de utilização das interfaces (bps e pps);

1.4.5.3.17. Suportar a rollback de configuração e imagem;

1.4.5.3.18. Possuir o registro local de eventos relevantes do sistema e suportar o envio via syslog de eventos relevantes ao sistema, com capacidade de configuração de múltiplos servidores de syslog;

1.4.5.3.19. Implementar rate limit da taxa logs enviados para servidores externos, com o objetivo de prevenir a sobrecarga e perda de logs por motivos de alta utilização de CPU, memória ou uso de banda;

1.4.5.3.20. Permitir reiniciar o equipamento pela interface gráfica e por CLI;

1.4.5.3.21. Implementar SNMPv1, SNMPv2c e SNMPV3;

1.4.5.3.22. Implementar traps SNMP;

1.4.5.3.23. Permitir a criação de MIBs customizadas;

1.4.5.3.24. Possuir suporte a monitoração utilizando RMON através de pelo menos 4 grupos: statistics, history, alarms e events

1.4.5.3.25. Possuir agente integrado de coleta e exportação de métricas de desempenho e eventos:

1.4.5.3.25.1. Coleta de métricas de desempenho compatível com Prometheus;

1.4.5.3.25.2. Coleta de métricas de desempenho em formato JSON utilizando cliente HTTP;

1.4.5.3.25.3. Exportação de métricas de desempenho compatíveis com, pelo menos, os sistemas AWS CloudWatch e S3, Azure Log Analytics e Application Insights, ElasticSearch, Fluentd,

GCP Cloud Monitoring e Logging, Graphite, Kafka, Splunk e StatsD;

1.4.5.3.25.4. Exportação de métricas de desempenho em formato JSON para um servidor HTTP;

1.4.5.3.25.5. Permitir definir critérios de inclusão e exclusão de coleta e exportação de métricas;

1.4.5.3.25.6. Deve incluir métricas de desempenho relacionadas a servidores virtuais, pool e pool members;

1.4.5.3.25.7. Deve incluir métricas de throughtput, conexões, bits, pacotes, disponibilidade;

1.4.5.3.25.8. Deve incluir métricas de requisições, respostas;

1.4.5.3.25.9. Deve incluir métricas de criptografia, incluindo cifras, algoritmos, versão, conexões, bytes criptografados, bytes descriptografados;

1.4.5.3.25.10. Deve incluir métricas de certificados digitais, incluindo data de expiração, issuer e subject;

1.4.5.3.25.11. Deve incluir métricas relacionadas a CPU, memória, discos e interfaces;

1.4.5.3.25.12. Deve incluir métricas de desempenho dos scripts de manipulação de tráfego, incluindo total de execuções, média de ciclos, máximo e mínimo de ciclos e falhas;

1.4.5.3.25.13. Deve incluir informações de inventário (hostname, id, versão, localização, plataforma, chassi, módulos provisionados);

1.4.5.3.25.14. Deve incluir métricas do cluster, incluindo data de sincronização;

1.4.5.3.25.15. Deve incluir informações de data da última configuração aplicada;

1.4.5.3.25.16. Deve possuir documentação pública do fabricante contendo informações de configurações, exemplos de configuração e modelos de mensagens;

1.4.5.3.26. Implementar debugging utilizando CLI via console e SSH;

1.4.5.3.27. Possuir ferramenta interna nativa de captura de tráfego de rede com informações contextuais da solução inseridas em cada pacote/frame;

1.4.5.3.28. Permitir a exportação de informações de diagnóstico, logs, configurações, desempenho para análises externas sem interferência na solução em produção. A análise deve ser feita em ferramenta, disponível sem custo adicional, online via web ou via aplicação para Windows, Linux ou MacOS;

1.4.5.3.29. Deve possuir suporte a Link Layer Discovery Protocol (LLDP), com, pelo menos, as informações: Port ID, TTL, Port Description, System Name, System Description, Management Address, Port VLAN ID, Port and Protocol VLAN ID, VLAN Name, Protocol Identity, Link Aggregation, Maximum Frame Size

1.4.5.3.30. Suportar exportação de informações de fluxos através sFlow, NetFlow, IPFIX ou outro protocolo similar;

1.4.5.3.31. Permitir a criação de códigos ou scripts capazes de manipular o tráfego, incluindo descartar, redirecionar, alterar, substituir e comparar valores e atributos, a partir de informações extraídas da conexão, sessão e protocolos;

1.4.5.3.32. Permitir utilizar listas de dados como fonte de dados por um script para validar se as conexões a serem estabelecidas obedecem a um dos critérios contidos nessa base de dados;

1.4.5.3.33. Implementar roteamento IPv4 e IPv6 estático e dinâmico:

1.4.5.3.33.1. Suportar a criação de múltiplos domínios de roteamento, com tabelas de rotas isoladas, em IPv4 e IPv6, BGP, OSPF e RIP em IPv4 e IPv6;

1.4.5.3.33.2. Permitir que cada domínio de roteamento utilize BGP, OSPF e RIP em IPv4 e IPv6;

1.4.5.3.33.3. Suportar integração via BGP para divulgação de prefixos;

1.4.5.3.33.4. Deve garantir que o retorno do tráfego seja encaminhado para o mesmo host que enviou o tráfego inicialmente para a solução, independente da configuração de rotas do equipamento. Por exemplo, no caso de múltiplos roteadores com acesso à Internet, a solução deve enviar o tráfego de retorno para o cliente sempre para o mesmo roteador que encaminhou o tráfego do cliente inicialmente para a solução;

1.4.5.3.33.5. Suportar Equal Cost Multipath (ECMP);

1.4.5.3.33.6. Implementar Bidirectional Forward Detection (BFD);

1.4.5.3.34. Implementar funções de entrega de aplicações através do balancear servidores com qualquer hardware, sistema operacional e tipo de aplicação:

1.4.5.3.34.1. Suportar os protocolos HTTP/1.0, HTTP/1.1, HTTP/2 e HTTP/3, para comunicação com o cliente e comunicação com o servidor;

1.4.5.3.34.2. Implementar a reutilização de conexões entre a solução e os servidores, para diferentes clientes e diferentes requisições;

1.4.5.3.34.3. Suportar os métodos de balanceamento round robin, least connections, weighted (por peso), tempo de resposta mais rápida baseado no tráfego real, baseado em parâmetros dinâmicos coletados via SNMP ou WMI;

1.4.5.3.35. Implementar criptografia de cookies;

1.4.5.3.36. Implementar persistência com pelo menos os métodos por cookie inserindo um novo cookie na sessão, por cookie utilizando um valor do cookie da aplicação, sem adição de cookie, por endereço IP destino, por endereço IP origem, por sessão SSL, parâmetros da URL acessada, parâmetro no header HTTP, qualquer informação do payload camada 7;

1.4.5.3.37. Permitir configuração de grupos de servidores secundários que devem ser utilizados para balanceamento somente quando uma quantidade mínima especificada de servidores estiver disponível no grupo primário. Caso o número de servidores disponíveis fique menor do que o especificado, a solução deve automaticamente distribuir o tráfego para o próximo grupo. Caso o número de servidores disponíveis volte ao valor mínimo, a solução deve automaticamente voltar a utilizar o grupo primário de servidores;

1.4.5.3.38. Permitir a replicação do tráfego destinado a servidores virtuais, permitindo habilitar a cópia do tráfego entre o cliente e a solução e entre a solução e o servidor;

1.4.5.3.39. Implementar pelo menos monitores de servidores de servidores via ICMP, conexões TCP e UDP pela respectiva porta no servidor e HTTP e HTTPS, incluindo HTTP/2;

1.4.5.3.40. Suportar balanceamento de carga de servidores SIP para VoIP;

1.4.5.3.41. Permitir limitar o número de conexões estabelecidas com cada servidor real;

1.4.5.3.42. Permitir limitar o número de conexões estabelecidas com cada servidor virtual;

1.4.5.3.43. Implementar Network Address Translation (NAT) do IP do servidor;

1.4.5.3.44. Implementar Network Address Translation (NAT) do IP do cliente;

1.4.5.3.45. Implementar proteção contra Denial of Service (DoS) em camada 3, 4 e 7;

1.4.5.3.46. Implementar proteção contra SYN floods;

1.4.5.3.47. Suportar servidores virtuais com endereço IPv4 e os servidores reais com endereços IPv6;

1.4.5.3.48. Suportar multiplexação TCP e reuso de sessão para reaproveitamento e uso eficiente de conexões entre a solução de balanceamento de aplicações e os servidores balanceados;

1.4.5.3.49. Suportar Stream Control Transmission Protocol (SCTP);

1.4.5.3.50. Implementar aceleração de TLS com instalação do certificado digital na solução, troca de chaves e criptografia dos dados;

1.4.5.3.50.1. Permitir recriptografar a conexão entre a solução e o servidor;

1.4.5.3.50.2. Permitir espelhamento de tráfego de conexões TLS;

1.4.5.3.50.3. Suportar diversas cifras e protocolos SSL/TLS, incluindo TLS 1, 1.1, 1.2, 1.3, Forward Secrecy/Perfect Forward Secrecy, RSA, ECDSA, DHE, ECDHE, AES-128, AES-256, CBC/GCM, Camellia128, Camellia256, SHA, SHA2 (SHA256/384) e ChaCha20-Poly1305;

1.4.5.3.51. Em relação ao tráfego TLS, deve suportar:

1.4.5.3.51.1. Autenticação do servidor pelo cliente, apresentando um certificado previamente configurado;

1.4.5.3.51.2. Autenticação do cliente pela solução, através da solicitação e verificação do certificado fornecido pelo cliente;

1.4.5.3.51.3. Autenticação mútua (mTLS), quando ambas as autenticações acima mencionadas ocorrem. Durante a autenticação com mTLS, a solução deve apresentar para o servidor um certificado de cliente com atributos extraídos do certificado original obtido do cliente, preservando a autenticação mútua fim a fim;

1.4.5.3.51.4. Encaminhar ao servidor real via cabeçalho HTTP todo o certificado utilizado pelo cliente para se autenticar;

1.4.5.3.51.5. Encaminhar ao servidor real via cabeçalho HTTP atributos específicos do certificado utilizado pelo cliente;

1.4.5.3.52. Suportar os algoritmos para sessões TLS:

1.4.5.3.52.1. SSL session cache Timeout;

1.4.5.3.52.2. Session Ticket;

1.4.5.3.52.3. OCSP (Online Certificate Status Protocol) Stapling;

1.4.5.3.52.4. Dynamic Record Sizing;

1.4.5.3.52.5. ALPN (Application Layer Protocol Negotiation);

1.4.5.3.52.6. Perfect Forward Secrecy;

1.4.5.3.53. Suportar múltiplos certificados digitais no mesmo servidor virtual, com identificação via SNI (Server Name Indication);

1.4.5.3.54. Suportar importação de certificados digitais e chaves privadas;

1.4.5.3.55. Possuir alertas visuais na interface web de certificados com vencimento próximo;

1.4.5.3.56. Implementar limpeza de cabeçalho HTTP;

1.4.5.3.57. Implementar compressão de conteúdo HTTP, suportar os algoritmos gzip e deflate e permitir definir compressão especificamente para certos tipos de objetos;

1.4.5.3.58. Permitir a criação de políticas para classificação de tráfego através de parâmetros da aplicação, incluindo informações de geolocalização IP, cabeçalhos de autenticação HTTP, cookies e

operações de cookie, cabeçalhos HTTP, host, método, Referer, Status Code e URI;

1.4.5.3.59. Permitir as ações para o tráfego classificado: bloqueio, reescrita e manipulação de URL, adicionar cabeçalho HTTP, redirecionar o tráfego para um servidor específico, escolher uma política de proteção web, logging do tráfego;

1.4.5.3.60. Suportar log de todas as sessões e permitir a customização do formato, incluindo endereço IP de origem, Porta TCP e UDP de origem, endereço IP de destino, porta TCP e UDP de destino, protocolo de camada 4 (TCP ou UDP), data e hora da mensagem, URL acessada;

1.4.5.3.61. Permitir utilizar diferentes configurações de envio de eventos de uma mesma aplicação, de forma que eventos válidos sejam enviados para um servidor e eventos de violações de segurança sejam enviados para outro servidor;

1.4.5.3.62. Permitir exportar eventos de acesso para servidores externos com configuração das informações exportadas;

1.4.5.3.63. Permitir a configuração de autenticação e autorização de clientes HTTP, através de base LDAP, RADIUS e certificados digitais;

1.4.5.3.64. Implementar integração com ambientes de orquestração de containers para criação dinâmica de serviços de entrega de aplicações e balanceamento de carga na solução, modificando a configuração de forma dinâmica e automática a partir de configurações feitas na plataforma de orquestração;

1.4.5.3.64.1. Suportar, pelo menos, as plataformas Kubernetes “Vanilla”, Red Hat OpenShift e VMware Tanzu;

1.4.5.3.64.2. Permitir a configuração através de ConfigMaps;

1.4.5.3.64.3. Permitir a configuração através de CustomResourceDefinition (CRD) da solução;

1.4.5.3.64.4. Permitir a configuração através de objetos de serviço (Service) do tipo LoadBalancer na plataforma;

1.4.5.3.64.5. Permitir a configuração através de objetos Ingress na plataforma;

1.4.5.3.64.6. Permitir a configuração através de objetos Route no OpenShift;

1.4.5.3.64.7. Permitir incluir serviços de entrega de aplicações da solução, tais como SSL Offload e proteção de aplicações;

1.4.5.3.64.8. O ADC deverá receber em tempo real as alterações do ambiente e atualizar automaticamente o pool de pods ou nodes disponíveis para o serviço publicado de acordo com a integração realizada;

1.4.5.3.65. Suportar o protocolo FTP com, pelo menos, as seguintes características:

1.4.5.3.65.1. Determinar os comandos FTP permitidos;

1.4.5.3.65.2. Requests FTP anônimos;

1.4.5.3.65.3. Validar conformidade com o protocolo FTP;

1.4.5.3.65.4. Proteger contra ataques de força bruta nos logins;

1.4.5.3.66. Suportar o protocolo SMTP com, pelo menos, as seguintes características

1.4.5.3.66.1. Limitar o número de mensagens;

1.4.5.3.66.2. Validar registro SPF do DNS;

1.4.5.3.66.3. Determinar quais métodos SMTP podem ser utilizados.

1.4.5.4. **Implementar proteção de aplicações no nível de rede e protocolo:**

1.4.5.4.1. Permitir implementação no modo que todo o tráfego seja bloqueado com exceções explícitas em regras de permissões e no modo que todo tráfego é permitido com exceções explícitas em regras de bloqueio;

1.4.5.4.2. Proteger de ataques DDoS nas camadas de rede e de sessão;

1.4.5.4.3. Proteger de ataques DDoS que utilizem SSL;

1.4.5.4.4. A solução deve permitir a criação de regras com, no mínimo, os parâmetros:

1.4.5.4.4.1. Endereço IP de destino

1.4.5.4.4.2. Endereço IP de origem

1.4.5.4.4.3. Porta de destino

5.4.4.4. Porta de origem

1.4.5.4.4.5. VLAN

1.4.5.4.4.6. Protocolo

1.4.5.4.4.7. Ação

1.4.5.4.4.8. Horário

1.4.5.4.4.9. Log;

1.4.5.4.4.10. Permitir definir agendamento para ativação da regra;

1.4.5.4.4.11. Permitir criar regras com base em zonas de segurança e por interface ou VLAN;

1.4.5.4.5. Implementar a descoberta automática de serviços presentes em objetos monitorados;

1.4.5.4.6. Permitir definir, no mínimo, as seguintes ações no tráfego:

1.4.5.4.6.1. Permitir: os pacotes são aceitos e passam pela solução;

1.4.5.4.6.2. Rejeitar: os pacotes são rejeitados e ocorre envio de pacotes de destino inatingível ou similar a origem do tráfego;

1.4.5.4.6.3. Descartar: onde os pacotes são descartados sem o envio de qualquer notificação a origem do tráfego;

1.4.5.4.7. Deve ser possível criar regras que sejam aplicadas em diferentes hierarquias, incluindo, no mínimo:

1.4.5.4.7.1. Global, regras válidas para todo o tráfego, independente da interface de ingresso;

1.4.5.4.7.2. Domínio de roteamento, regras válidas para todo o tráfego daquele domínio, independente da interface de ingresso;

1.4.5.4.7.3. Objeto, regras válidas para objetos específicos;

1.4.5.4.8. Deve possuir criptografia IPSEC para comunicação entre sites;

1.4.5.4.9. Permitir a configuração de alertas que informem automaticamente sobre ataques e anomalia de tráfego, através de limiares baseados no perfil de rede ou através de limites de tráfego atingido;

1.4.5.4.10. Permitir a restauração das configurações de proteções originais;

1.4.5.4.11. Deve permitir criar lista de exceção de regras por endereço IP específico ou faixa de sub-

rede;

1.4.5.4.12. Permitir a criação de códigos ou scripts para customizar e aumentar o nível de segurança contra DDoS;

1.4.5.4.13. Permitir o consumo de listas externas de IPs para bloqueio com base em destino e origem, com atualização automática e ajuste manual da frequência de atualização;

1.4.5.4.14. Permitir o acionamento via API do descarte de conexões (shun) para integração com terceiros, tais como SIEM, IPS, IDS e outros;

1.4.5.4.15. Permitir a criação de regras de filtragem através de API REST declarativa;

1.4.5.4.16. A documentação da API deve ser pública;

1.4.5.4.17. Exibir uma lista de proteções ativas juntamente com estatísticas resumidas sobre as quantidades de tráfego descartado e aceito

1.4.5.4.18. Incluir informações estatísticas sobre o tráfego total e o total bloqueado por cada tipo de prevenção;

1.4.5.4.19. Implementar proteção contra pacotes inválidos, incluindo verificação para DNS malformed, Bad ICMP Frame, Bad ICMP Checksum, ICMP Frame too Large, BadIGMP Frame, Bad IP TTL Value, Bad IP Version, Header Length Too Short, Bad Source, Bad IPV6 Hop Count, Bad IPV6 Version, Bad TCP Checksum, Bad TCP Flags, SYN & FIN Set, Bad UDP Checksum, ARP Flood, ICMPv4 Flood, ICMPv6 Flood , IGMP Flood, IGMP Fragment Flood, TCP RST Flood, TCP SYN ACK Flood, TCP SYN Flood, UDP Flood, SIP ACK Method, SIP Malformed, Single Endpoint Flood, Single Endpoint Sweep, LAND Attack, DNS Water-torture e fornecer estatísticas para os pacotes descartados;

1.4.5.4.20. Implementar descarte de sessões TCP ociosas se o cliente não enviar uma quantidade de dados dentro de um período configurável;

1.4.5.4.21. Limitar o número de consultas DNS por segundo através da configuração de limiares;

1.4.5.4.22. Mitigar, no mínimo, os tipos de ataques ICMP/UDP/TCP Flood, TCP Flag Abuse, GET/POST Flood, SYN Flood, UDP Bandwidth Attack, Smurfing, NTP Reflection Attack, TCP/UDP
Bandwidth Attack, Fragging Attack, Slowloris, Connection Attack e Fragmentation Attacks;

1.4.5.4.23. Possuir recurso de bloqueio automático e temporário de atacantes, devendo ser possível especificar o tempo mínimo para iniciar o bloqueio e o tempo de bloqueio;

1.4.5.4.24. Suportar envio de SNMP traps para cada ataque DoS detectado;

1.4.5.4.25. Possuir uma ferramenta de teste de pacotes, através da qual deve ser possível realizar testes de pacotes;

1.4.5.4.26. Deve possuir a funcionalidade de limiares automático para vetores de DoS:

1.4.5.4.26.1. Essa funcionalidade deve valer tanto para proteção geral como também para proteção de serviços específicos.

1.4.5.4.27. Os limiares automáticos serão construídos pelo próprio sistema e aplicados aos diversos vetores de ataques selecionados;

1.4.5.4.28. Permitir configurar o sistema para detectar e mitigar assinaturas dinâmicas, capaz de detectar possíveis ameaças de DoS baseado no histórico e comportamento do tráfego e mitigar automaticamente essas ameaças;

1.4.5.4.29. Suportar integração com serviço de tratamento de DDoS externo através do compartilhamento de informação de vetores e sinalização de ataques em andamento para

redirecionamento de tráfego via BGP e limpeza do tráfego em centros de limpezas externos;

1.4.5.5. **Implementar serviços de entrega de aplicações distribuídas através do serviço de DNS:**

1.4.5.5.1. Implementar serviços de DNS com as funções de DNS autoritativo, DNS secundário, DNS resolver, DNS cache e balanceamento de servidores de DNS;

1.4.5.5.2. Implementar DNSSec, independente da estrutura dos servidores DNS em uso;

1.4.5.5.3. Implementar transferência de zonas para múltiplos servidores DNS primários responsáveis por diferentes zonas;

1.4.5.5.4. Suportar uso de chave criptográfica TSIG para comunicação segura entre servidores DNS, obedecendo no mínimo os padrões HMAC MD5, HMAC SHA-1 ou HMAC SHA-256;

1.4.5.5.5. Implementar offload dos servidores de DNS, funcionando como o DNS secundário;

1.4.5.5.6. Implementar proteções contra-ataques DNS, incluindo no mínimo a inspeção de protocolo, validação de protocolo, UDP flood, pacotes malformados, teardrop e DNS Water-torture;

1.4.5.5.7. Permitir a criação de códigos ou scripts que possam manipular as respostas de DNS;

1.4.5.5.8. Implementar filtragem de pacotes e tipos de requisições;

1.4.5.5.9. Implementar segurança do protocolo DNS, protegendo de ataques de negação de serviço, NXDOMAIN, reflexão e amplificação de DNS e Cache Poisoning;

1.4.5.5.10. Implementar stateful inspection das requisições e respostas de DNS;

1.4.5.5.11. Possuir base de geolocalização IP;

1.4.5.5.12. Implementar DNS64 e implementar as seguintes integrações:

1.4.5.5.12.1. Cliente envia consulta AAAA, a solução encaminha a consulta (recursivo) com A e AAAA e responde com um prefixo + A e AAAA

1.4.5.5.12.2. Cliente envia consulta AAAA, a solução encaminha a consulta (recursivo) com A, caso não tenha resposta, faz a consulta com AAAA, responde para o cliente um prefixo + A e
AAAA

1.4.5.5.12.3. Cliente envia consulta AAAA, a solução encaminha uma consulta (recursivo) como A e responde um prefixo + AAAA

1.4.5.5.13. Implementar filtros para tipos de requisição, de forma que apenas as operações e requisições autorizadas sejam encaminhadas para os servidores de DNS.

1.4.5.5.14. Suportar pelo menos os tipos de requisição SOA, A, AAAA, CNAME, DNAME, HINFO, MX, NS, PTR, SRV e TXT;

1.4.5.5.15. Suportar DNS over HTTPS (DoH);

1.4.5.5.16. Permitir a criação de resoluções de DNS com tratamento diferenciado de consultas conforme origem das requisições;

1.4.5.5.17. Apresentar estatísticas sobre consultas de DNS por aplicação, nome da query, tipo da query, endereço IP do cliente;

1.4.5.5.18. Implementar modo inline na estrutura de DNS existente e transparente;

1.4.5.5.19. Suportar IP Anycast;

1.4.5.5.20. Implementar alta disponibilidade sem depender de BGP ou outro protocolo de roteamento;

1.4.5.5.21. Implementar alta disponibilidade de Data Centers e serviços baseada em respostas a requisições DNS, de forma que a resposta a requisições DNS devem conter apenas endereços que estejam disponíveis no momento, e balanceadas por usuário, de acordo com as políticas definidas;

1.4.5.5.22. Suportar resolução de nomes baseada em topologia, onde requisições de DNS são respondidas baseado no país, continente, ou endereço IP de onde veio a requisição;

1.4.5.5.23. Suporte a monitoração de estado de saúde de servidores, serviços e links de conexão a provedor de serviço, garantindo a disponibilidade do serviço oferecido;

1.4.5.5.24. Suportar monitores utilizando HTTPS, incluindo a validação do SNI;

1.4.5.5.25. Suportar pelo menos os algoritmos de balanceamento Round Robin, Global Availability, Ratio, LDNS Persist, Geografia, round trip time e hops;

1.4.5.5.26. Implementar persistência da conexão do usuário entre aplicações ou data centers;

1.4.5.5.27. Suportar o controle de grupos de aplicações, e permitir que um usuário seja redirecionado para outro datacenter quando houver falha em qualquer das aplicações de um mesmo grupo;

1.4.5.5.28. Permitir que as políticas sejam configuradas individualmente por aplicação que será balanceada;

1.4.5.5.29. Permitir que a contingência seja automática;

1.4.5.5.30. Permitir o retorno do Data Center de forma automática e manual;

1.4.5.5.31. A solução deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com IPv4 (requisições AAAA);

1.4.5.5.32. Possuir suporte a IPv6 no balanceamento global entre datacenters;

1.4.5.5.33. Possuir a funcionalidade de resposta rápida a requisições de DNS, permitindo respostas mais rápidas para zonas que seja autoritativo;

1.4.5.5.34. Suportar Response Policy Zones (RPZ), mecanismo de proteção de resolução para DNS recursivo que permite o tratamento customizado da resolução de nomes, capaz de filtrar queries DNS para domínios considerados maliciosos e retornar respostas customizadas;

1.4.5.5.35. Suportar EDNS-Client-Subnet (ECS) para tanto responder requisições de clientes para balanceamento de Data Center ou encaminhar requisições de clientes.

1.4.5.5.36. Implementar a utilização da subnet do cliente presente no ECS para tomada de decisão de balanceamento de Data Center, independente do endereço do LDNS;

1.4.5.5.37. Suportar inserir o ECS para outros servidores DNS;

1.4.5.5.38. A solução deve fazer persistência baseado no endereço IP do cliente (ECS), significando que se o cliente mudar de LDNS resolver, deve ser usada a persistência existente para manter o cliente no mesmo Data Center;

1.4.5.5.39. Permitir consultar a resposta de uma resolução de DNS em uma base de IP e permitir que a resposta seja alterada antes de ser enviada para o cliente;

1.4.5.5.40. Registrar todas as tentativas de comunicação com os nomes de domínio que hospedem conteúdo malicioso, incluindo IP de origem, destino, data e hora do acesso.

1.4.5.5.41. Suportar, no mínimo, as ações de apenas registrar, bloquear o dado ou substituir o nome do domínio;

1.4.5.5.42. Permitir configurar rate limit realizadas via TCP ou UDP por FQND;

1.4.5.5.43. Permitir configurar rate limit para consultas realizadas via TCP ou UDP por IP de origem;

1.4.5.6. **Implementar proteção para aplicações web e API contra ameaças na camada de aplicação:**

1.4.5.6.1. Possuir tecnologia para mitigação de DDoS em camada 7 a partir de análises comportamentais;

1.4.5.6.2. Implementar ajustes automáticos e adaptativos de limiares de DoS;

1.4.5.6.3. Permitir a captura automática do tráfego relativo a ataques DoS em camada 7, web scraping e força bruta;

1.4.5.6.4. Implementar proteção para aplicações web contra ameaças listadas no OWASP Top 10 2021;

1.4.5.6.5. Implementar modelo positivo de segurança de aplicações web;

1.4.5.6.6. Implementar modelo negativa de segurança, ou seja, adotar assinatura de ataques, ameaças e exploração de vulnerabilidade, de aplicações web;

1.4.5.6.7. Possuir conjuntos de configurações de segurança pré-definidas para configuração rápida de políticas;

1.4.5.6.8. Permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;

1.4.5.6.9. Permite configurar de forma granular, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies;

1.4.5.6.10. Permitir desativar a inspeção para URL específicas;

1.4.5.6.11. Implementar identificação do usuário da aplicação web, mantendo a identificação até que o usuário tenha deixado o aplicativo;

1.4.5.6.12. Permitir a integração com firewall de banco de dados;

1.4.5.6.13. Suportar aplicações que utilizam protocolo WebSocket;

1.4.5.6.14. Suportar os protocolos HTTP/1.0, HTTP/1.1 e HTTP/2.0, para comunicação com o cliente e comunicação com o servidor, sem a necessidade de downgrade de versão;

1.4.5.6.15. Implementar proteção contra:

1.4.5.6.15.1. Acesso por força bruta;

1.4.5.6.15.2. DoS e DDoS em camada 7;

1.4.5.6.15.3. Buffer Overflow;

1.4.5.6.15.4. Cross Site Request Forgery (CSRF);

1.4.5.6.15.5. Cross-Site Scripting (XSS);

1.4.5.6.15.6. Server-Side Request Forgery (SSRF);

1.4.5.6.15.7. SQL Injection;

1.4.5.6.15.8. Parameter tampering;

1.4.5.6.15.9. Cookie poisoning;

1.4.5.6.15.10. HTTP Request Smuggling;

1.4.5.6.15.11. Manipulação de campos escondidos (hidden input);

1.4.5.6.15.12. Manipulação de cookies;

1.4.5.6.15.13. Roubo de sessão através de manipulação de cookies;

1.4.5.6.15.14. Sequestro de sessão;

1.4.5.6.15.15. Validação de consistência de formulários;

1.4.5.6.15.16. Validação do cabeçalho do “user-agent” para identificar clientes inválidos;

1.4.5.6.16. Permitir especificar quais URLs devem ser utilizadas para proteção contra CSRF (Cross-Site Request Forgery);

1.4.5.6.17. Suportar codificação HTML "application/x-www-form-urlencoded";

1.4.5.6.18. Suportar HTTP Batched Request com proteções e assinaturas considerando individualmente URIs, cabeçalhos e conteúdo;

1.4.5.6.19. Suportar codificação fragmentada (chunked encoding);

1.4.5.6.20. Suportar validações de protocolo:

1.4.5.6.20.1. Restrição de métodos;

1.4.5.6.20.2. Restrição de protocolos e versões;

1.4.5.6.20.3. Validação de conformidade com RFCs;

1.4.5.6.20.4. Validação de caracteres URL-encoded;

1.4.5.6.20.5. Validação de codificação fora de padrão %uXXYY.

1.4.5.6.21. Suportar validações de HTML com nome de parâmetros, tamanho e tipo dos valores de parâmetros e combinação de nome, tipo e tamanho de parâmetros;

1.4.5.6.22. Possuir técnicas de detecção de evasões:

1.4.5.6.22.1. URL-decoding;

1.4.5.6.22.2. Terminação Null Byte String;

1.4.5.6.22.3. Paths autorreferenciados;

1.4.5.6.22.4. Case de caracteres misturados;

1.4.5.6.22.5. Uso excessivo de espaços em branco;

1.4.5.6.22.6. Decodificação de entidades HTML;

1.4.5.6.22.7. Caracteres de escape;

1.4.5.6.23. Permitir a inspeção externa de arquivos enviados por usuários (upload) para os servidores de aplicação utilizando Internet Content Adaptation Protocol (ICAP);

1.4.5.6.24. Capacidade de filtrar cabeçalhos, corpo e status de respostas;

1.4.5.6.25. Permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle;

1.4.5.6.26. Implementar validação de URL;

1.4.5.6.27. Validação de métodos HTTP utilizados (GET, POST, HEAD, OPTIONS, PUT, TRACE, DELETE, CONNECT) por URL;

1.4.5.6.28. Implementar proteção de aplicações web que utilizam chamadas de API, protegendo tanto a aplicação como a API, com a visibilidade que se trata da mesma sessão de usuário;

1.4.5.6.29. Suportar aplicações Single-Page Application (SPA);

1.4.5.6.30. Permitir a customização da resposta de bloqueio;

1.4.5.6.31. Permitir a configuração de lista de exceções temporárias ou permanentes de endereços IP bloqueados;

1.4.5.6.32. Permitir adicionar, automaticamente e manualmente, em uma lista de bloqueio, os endereços IP de origem que ultrapassarem limites estabelecido, por um período configurável;

1.4.5.6.33. Implementar as proteções:

1.4.5.6.33.1. Proteção contra exposição de informações do ambiente e servidores internos como, sistema operacional e servidor web;

1.4.5.6.33.2. Ocultar qualquer mensagem de erro HTTP dos usuários;

1.4.5.6.33.3. Remover as mensagens de erro às páginas que serão enviadas aos usuários;

1.4.5.6.34. Suportar políticas por geolocalização para restrição de acesso a determinados países;

1.4.5.6.35. Implementar aprendizado automático para identificação da estrutura da aplicação, incluindo URLs, parâmetros URLs, campos de formulários, tipo de dado, tamanho de caracteres, cookies;

1.4.5.6.36. O aprendizado deve ser capaz de diferenciar atributos com o mesmo nome, mas presentes em URLs diferentes;

1.4.5.6.37. Implementar aprendizado automático de XML;

1.4.5.6.38. Permitir a importação de arquivo de esquema XML;

1.4.5.6.39. Implementar aprendizado automático de JSON;

1.4.5.6.40. Permitir a importação de arquivo de esquema JSON;

1.4.5.6.41. Permitir a criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real;

1.4.5.6.42. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;

1.4.5.6.43. Implementar detecção e mitigação de ameaças e ataques com base em assinaturas de ataques, com atualização periódica e automática da base de assinaturas;

1.4.5.6.44. As assinaturas devem ser atualizadas durante o período do contrato, sem custo adicional;

1.4.5.6.45. Não serão aceitas soluções que definem assinaturas como sendo uma base de reputação de IP;

1.4.5.6.46. A atualização deve ser relacionada apenas as assinaturas, não sendo aceitas soluções que demanda a atualização do sistema operacional para atualização de cada nova versão da base de assinaturas;

1.4.5.6.47. Permitir a configuração automática de assinaturas com base em uma lista interna de tecnologias utilizadas pela aplicação;

1.4.5.6.48. Permitir desabilitar assinaturas específicas para determinados parâmetros, se comportando como exceção da configuração geral da política;

1.4.5.6.49. Permitir configurar um período de adaptação de novas assinaturas, quando nenhuma requisição que viole a assinatura deve ser bloqueada, apenas informada em relatório. Este processo deve ser automático, não sendo necessário a criação de regras específicas a cada atualização de assinatura;

1.4.5.6.50. Possuir assinaturas de ataques para conteúdo em JSON e XML;

1.4.5.6.51. Possuir proteções contra XML Bomb;

1.4.5.6.52. Possuir proteção para WebServices, suportar WS-I Basic Profile, importação de WSDL e aplicação de controles, criptografar e descriptografar partes das mensagens SOAP, assinar digitalmente e verificar de partes das mensagens SOAP;

1.4.5.6.53. Possuir integração com soluções externas de análise vulnerabilidade para importação de relatórios e configuração de políticas de segurança, indicando quais vulnerabilidades podem ser resolvidas e quais devem ser resolvidas manualmente externamente;

1.4.5.6.54. Implementar detecção de DoS na camada 7, através de análise comportamental, com aprendizado automático do comportamento da aplicação e combinação com nível de carga do servidor;

1.4.5.6.54.1. Permitir apenas registrar o ataque, sem tomar nenhuma ação de bloqueio;

1.4.5.6.54.2. Implementar detecção com base no número de requisições por segundo enviados a uma URL específica;

1.4.5.6.54.3. Implementar detecção com base no número de requisições por segundo enviados de um IP específico;

1.4.5.6.54.4. Implementar detecção com base na validação do cliente através de código executado no navegador para identificação de bots;

1.4.5.6.54.5. Implementar detecção com base no aumento de um determinado percentual do número de transações por segundo (TPS);

1.4.5.6.54.6. Implementar detecção com base no aumento de carga e latência do servidor de aplicação;

1.4.5.6.54.7. Implementar detecção com base no número máximo de transações por segundo de um determinado IP;

1.4.5.6.55. Implementar mitigações para ataques DoS, incluindo resolução de CAPTCHA, descarte de todas as requisições de um determinado IP, descarte por geolocalização IP, injeção de um desafio JavaScript para detectar se é um usuário legítimo ou bots;

1.4.5.6.56. Implementar mitigação de ataques DDoS através de assinaturas dinâmicas em tempo real para proteção da aplicação;

1.4.5.6.57. Implementar detecção e mitigação de ataques de força bruta de usuário/senha em páginas de login, com configuração da quantidade máxima de tentativas e tempo de mitigação;

1.4.5.6.57.1. Identificar ataques com diferentes usuários e mesma origem;

1.4.5.6.57.2. Identificar ataques com diferentes origens e mesmo usuário;

1.4.5.6.57.3. Identificar ataques de forma global, considerando a quantidade de tentativas e implementando contramedidas de forma global para a política;

1.4.5.6.58. Possuir funcionalidade para integração com listas externas de credenciais expostas para mitigar ataques Credential Stuffing e Password Sprawl;

1.4.5.6.59. Implementar mitigação através de listas de bloqueio dinâmica de endereços IPs após validação sem sucesso de desafios e permitir a configuração do tempo de bloqueio;

1.4.5.6.60. Implementar mitigação através de listas de bloqueio dinâmica de endereços IPs que ultrapassem um número máximo de violações por minuto e permitir a configuração do tempo de bloqueio;

1.4.5.6.61. Implementar detecção e mitigação para proteção contra bots através da combinação de

desafios enviados ao navegador do usuário e técnicas avançadas de análise;

5.6.61.1. Não serão aceitas soluções que utilizam apenas o user-agent para detecção de bots;

1.4.5.6.62. Implementar proteção proativa de ataques automatizados por bots e outras ferramentas, como web scrapers.

1.4.5.6.63. Possuir atualização automática de definição de bots;

1.4.5.6.64. Permitir a configuração de bloqueio e permissão de bots benignos conhecidos, como Google, Yahoo! e Microsoft Bing;

1.4.5.6.65. Permitir a criação de definições de bots;

1.4.5.6.66. Implementar proteção de APIs através da imposição de regras de endpoint e métodos permitidos;

1.4.5.6.67. Permitir a configuração de quotas e rate limits para chamadas em APIs de forma global na política;

1.4.5.6.68. Permitir a configuração de quotas e rate limits para chamadas em APIs por endpoint;

1.4.5.6.69. Permitir configurar exceções as regras de rate limits para chamadas na API;

1.4.5.6.70. Implementar proteção de conteúdo no formato JSON (JavaScript Object Notation);

1.4.5.6.71. Suportar proteção de conteúdo de mensagens no formato GraphQL, incluindo assinaturas de ataques, profundidade de query, GraphQL batching, inspeção de conteúdo JSON em mensagens POST e GET;

1.4.5.6.72. Suportar importação de especificação de API compatível com OpenAPI v2 e v3, nos formatos YAML ou JSON, com suporte a parâmetros no path e importação de respostas;

1.4.5.6.73. Implementar funcionalidade de autenticação e autorização de clientes de API utilizando, pelo menos, os métodos HTTP Basic e OAuth 2.0;

1.4.5.6.74. Implementar funcionalidade para prevenir vazamento de informações, dados sensíveis e outros tipos de dados confidenciais, sigilosos ou restrito, através do bloqueio ou remoção dos dados confidenciais;

1.4.5.6.75. Implementar funcionalidades para prevenir vazamento de dados sensíveis em mensagens de erro HTTP, códigos das aplicações, entre outros, retirando os dados ou mascarando a informação nas páginas enviadas aos usuários;

1.4.5.6.76. Implementar funcionalidade para ocultar erros de aplicação ou infraestrutura do usuário;

1.4.5.6.77. Permitir a configuração de fluxo de navegação da aplicação, de forma que um usuário só pode alcançar determinada URL se passar por outras anteriormente;

1.4.5.6.78. Permitir a correção de um falso positivo através da aceitação da requisição e atualização da política de forma automática;

1.4.5.6.79. Possuir um nível severidade de violação de múltiplos níveis para fácil identificação de violações de maior e menor prioridade;

1.4.5.6.80. Implementar um identificador único para cada requisição tratada pela solução;

1.4.5.6.81. Permitir o armazenamento local de eventos e exportação para servidores externos;

1.4.5.6.82. Permitir configurar a retenção dos eventos por tempo e volume;

1.4.5.6.83. Implementar a detecção, remoção ou codificação de dados sensíveis dos eventos como, por exemplo, números de cartão de crédito, CPF e senhas;

1.4.5.6.84. Implementar a criptografia de parâmetros específicos da aplicação, tais como credenciais e dados sensíveis, sem a necessidade de atualizar a aplicação. Esta criptografia de dados deve ser implementada no payload do HTTP, ou seja, nos dados propriamente ditos e não apenas via protocolo de transporte/túnel (TCP/TLS);

1.4.5.6.85. Implementar a ofuscação do nome de um parâmetro sensível da aplicação utilizando caracteres aleatórios, devendo ser mudado frequentemente pela solução para dificultar ataques direcionados;

1.4.5.6.86. Possuir API REST para configuração de servidores virtuais, políticas de segurança, parâmetros, perfis e demais configurações;

1.4.5.6.87. Permitir exportar as políticas de segurança para arquivos texto, JSON ou XML;

1.4.5.6.88. Possuir integração com esteiras de automação que permita que as configurações sejam realizadas de forma automática e dinâmica, de forma declarativa, por ferramentas de automação e orquestração, permitindo que a solução seja integrada ao ciclo de desenvolvimento;

1.4.5.7. Suportar integração com funcionalidade de gestão avançada de tráfego automatizado para detecção e mitigação de ataques, abusos e fraudes, com detecção de tráfego gerado por usuários, bots benignos e malignos, através de telemetria de uso coletada da aplicação, sem a utilização de CAPTCHAs ou desafios para o navegador;

1.4.5.7.1. Implementar funcionalidade de forma nativa na solução ou possuir integração com serviço em nuvem do mesmo;

1.4.5.7.2. Implementar proteção de aplicações web, de dispositivos móveis e APIs;

1.4.5.8. **Software e licenciamento**

1.4.5.8.1. Todas as licenças que compõem a solução deverão ser de propriedade da CONTRATANTE e permitir a plena continuidade de utilização e operação da solução mesmo após o término do contrato, de forma perpétua.

1.4.5.8.2. As assinaturas da solução de WAF devem ser atualizadas durante o período do contrato sem que seja necessário nenhum custo adicional por parte da CONTRATANTE na aquisição de novas licenças ou subscrições.

1.4.5.9. **Instalação e configuração**

1.4.5.9.1. O serviço de instalação e configuração deverá ser executado por técnico certificado pelo fabricante.

1.4.5.9.2. O serviço de instalação compreende as atividades de planejamento, instalação física, instalação lógica e finalização da solução no ambiente da CONTRATADA.

1.4.5.9.3. O serviço de configuração consiste em ajustar todos os parâmetros necessários (físicos e lógicos) para o funcionamento da solução e a sua adequação para funcionamento no ambiente da CONTRATADA atendendo aos requisitos dessa especificação.

1.4.5.9.4. Após o serviço de instalação, a contratada deve ministrar o treinamento do tipo hands-on, com todo repasse de conhecimento da configuração implementada e principais funcionalidades.

1.4.5.10.**Suporte, manutenção e atualização de versão**

1.4.5.10.1. O suporte técnico compreende o diagnóstico e identificação de problemas, apoio técnico na utilização, correção de erros, defeitos (bugs) ou mau funcionamento sobre qualquer funcionalidade, recurso, componente ou módulo disponível de forma nativa na solução de WAF e balanceamento, ou decorrente de qualquer adaptação (customização) e ajuste (tuning) efetuada pelo fabricante da solução.

1.4.5.10.2. O atendimento a um chamado de suporte deverá ocorrer por qualquer uma das seguintes formas: contato telefônico, envio de mensagem eletrônica (e-mail), acesso ao sítio (website) do fabricante da solução de WAF, com controle de acesso por senha fornecida pela Contratada.

1.4.5.10.3. O atendimento telefônico sempre que aplicável e viável, por meio de ligação local em Belo Horizonte/MG ou ligação interurbana gratuita (0800) e deverá ter um único número de contato

para todos os produtos de software que compõem a solução de WAF.

1.4.5.10.4. A CONTRATANTE poderá efetuar um número ilimitado de chamados técnicos para o fabricante, por qualquer uma das formas disponíveis, durante vigência do contrato vinculado a este edital.

1.4.5.10.5. O fornecedor ou Assistência Técnica Autorizada ou Revendedor Credenciado deverá retornar, via e-mail, a confirmação da abertura do chamado técnico, doravante denominado confirmação do chamado, contemplando as seguintes informações na sua abertura.

1.4.5.10.6. O atendimento ao chamado técnico deverá ocorrer pelo menos por uma das seguintes formas:

chamada telefônica, envio de mensagem eletrônica (e-mail), recursos disponíveis no sítio (site) do fabricante da solução de WAF por acesso remoto fornecido pela Contratada.

1.4.5.10.7. Um chamado técnico somente será considerado contingenciado ou concluído com o aceite da CONTRATANTE, na forma de um visto na ordem de serviço correspondente ou aceite por e-mail ou ainda, diretamente no sistema oferecido pelo fabricante, caso esta forma seja utilizada.

1.4.5.10.8. Deverá ser garantido à CONTRATANTE o pleno acesso ao sítio (site) dos fabricantes dos produtos que compõem a solução de WAF, com direito a consultas a quaisquer bases de conhecimentos e fóruns de discussão disponíveis para seus usuários.

1.4.5.10.9. Caberá exclusivamente à CONTRATANTE a decisão de implantar ou não quaisquer atualizações de software fornecidos pelo suporte do fabricante.

1.4.5.10.10. A CONTRATADA deverá disponibilizar mecanismos para a atualização de software pelo download direto através da própria aplicação, pelo envio das mídias ou através de download no seu sítio (site) ou do fabricante do software em questão.

1.4.5.10.11. A atualização de software é uma alteração da versão anterior com o objetivo de implementar melhorias. Essas melhorias podem ser de usabilidade, correção de falhas, desempenho, adição de novas funcionalidades, etc.

1.4.5.10.12. O prazo de atualização de todo software fornecido deve ser igual ao período de garantia do produto. Durante a vigência do contrato, a CONTRATANTE terá direito a todas atualizações de versão e release dos softwares.

1.4.5.11.**Garantia**

1.4.5.11.1. Os produtos que compõe(m) a solução devem estar em linha de fabricação até a data de assinatura do contrato e a data de final de suporte (end-of-support) deve ser após termino do contrato desta solução.

1.4.5.11.2. O serviço de Garantia contempla garantir o correto e pleno funcionamento de todos os itens adquiridos, seja hardware, software e os componentes necessários para o funcionamento da solução.

1.4.5.11.3. A CONTRATADA deverá garantir a substituição de qualquer módulo defeituoso, incluindo hardware, software ou componentes necessários para o funcionamento da solução durante o prazo contratado; bem como o próprio equipamento se for necessário.

1.4.5.11.4. Não haverá custos adicionais para a CONTRATANTE de substituição de quaisquer componentes durante o período de garantia.

1.4.5.11.5. Pazo de garantia deverá ser de 60 meses.

1.4.5.12. Documentação para avaliação:

1.4.5.12.1. Junto ao envio da proposta comercial, na sessão do pregão, a empresa licitante deverá enviar: datasheets, manuais ou guias de administração da solução de segurança de datacenter, para fins de avaliação técnica, sob pena de desclassificação.

1.4.5.12.2. Junto ao envio da proposta comercial, na sessão do pregão, a empresa licitante deverá enviar documento comprobatório de ser parceira credenciada do fabricante da solução de segurança de datacenter, sob pena de desclassificação.

1.4.6. Serviço de Instalação e Configuração dos Equipamentos

1.4.6.1. Os serviços de instalação e configuração da solução serão executados no local definido da CONTRATANTE.

1.4.6.2. A CONTRATADA deverá realizar os serviços de instalação e configuração dos equipamentos e licenciamentos de softwares de forma a garantir o seu pleno funcionamento.

1.4.6.3. A CONTRATADA deverá garantir todos os equipamentos, componentes, acessórios e cabos de conexão para interligar fisicamente todos os componentes das soluções entregues.

1.4.6.4. Todas as configurações serão realizadas em conformidade com a recomendação dos fabricantes dos equipamentos e softwares das soluções ofertadas, conforme melhores práticas de implementação recomendadas pelos fabricantes.

1.4.6.5. Todos os equipamentos adquiridos na solução deverão ser instalados, configurados e testados.

1.4.6.6. No datacenter, migração de 22 (vinte e duas) maquinas virtuais do atual ambiente legado da DINT em Hyper-V para a nova infraestrutura hiperconvergente, totalizando 20TB de volume de dados.

1.4.6.7. Treinamento hands-on:

1.4.6.7.1. Este repasse de conhecimento visa fornecer à equipe da CONTRATANTE a capacidade de operar o ambiente hiperconvergente instalado. Devem ser contempladas pelo menos 16 horas para o ambiente de datacenter (hiperconvergência e backup), e pelo menos 16 horas para o ambiente de segurança de informação (Firewall de Perímetro e Solução de Segurança de Datacenter);

1.4.6.8. Documentação:

1.4.6.8.1. Após implementação e validação do cluster e do ambiente de segurança da informação, deverá emitido a documentação “As Built” contendo todas as configuração e documentos comprobatórios do sucesso da instalação, parametrização do ambiente, licenças e versões;

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

A infraestrutura computacional da PMMG possui alto nível de complexidade de administração, especialmente no que tange ao provisionamento, integração, disponibilidade, flexibilidade, proteção de dados, gerenciamento centralizado e segurança das informações, provocando impactos diretos no bom atendimento das crescentes demandas por novos serviços.

A infraestrutura tecnológica, que sustenta as aplicações e serviços de TI, utiliza-se de diversas soluções de hardware e software para sua composição e funcionamento, sendo necessária a constante manutenção e atualização deste parque de modo a manter a compatibilidade e o nível de suporte técnico adequado a necessidade, além do acesso a novos recursos.

Tendo em vista que, a solução de processamento e armazenamento das informações, em uso atualmente PMMG, encontram-se fora de garantia/suporte, operando de forma ininterrupta há mais de 10 anos, naturalmente, ocorre uma defasagem tecnológica, além do fim do suporte prestado pelo fabricante, sem a possibilidade de renovação.

A contratação da Solução de Tecnologia Hiperconvergente, se justifica tanto pelas ações necessárias ao atendimento do PDTI da PMMG nos anos 2023/2024, que buscam a melhoria contínua dos serviços de TI, identificar novas tecnologias alinhadas a necessidade de inovação, identificar melhorias na infraestrutura de Data Center, aprimorar a solução de segurança da informação, e, assim, propor um parque

tecnológico adequado e necessário para suportar as demandas do CONTRATANTE; quanto pela necessidade de expansão do ambiente tecnológico, por meio da aquisição de recursos computacionais de qualidade, visando a disponibilidade dos equipamentos no parque tecnológico, substituindo aqueles já depreciados em função do uso prolongado e obsolescência.

Objetivando a sustentação dos produtos e serviços de TI demandados pela PMMG, faz-se necessária a aquisição de equipamentos de informática, nos quantitativos, custos e modelo de prestação, por meio da modernização da Solução de Tecnologia existente, compreendendo equipamentos de comunicação de dados, armazenamento e processamento e softwares de gerenciamento, por apresentar as melhores características de tecnologia, economia e consumo, necessárias para atender as demandas da PMMG.

3. REQUISITOS DA CONTRATAÇÃO

3.1. **Da participação de consórcios:**

3.1.1. Será permitida a participação de empresas reunidas em consórcio.

3.2. **Da Subcontratação:**

3.2.1. É admitida a subcontratação parcial do objeto, limitada a 25% do serviço a ser executado

3.3. **Da Sustentabilidade:**

3.3.1. Os critérios de sustentabilidade da contratação devem ser atendidos de acordo com os seguintes requisitos:

3.3.1.1. Não serão exigidos critérios de sustentabilidade na presente contratação, considerando o Estudo Técnico Preliminar

3.4. **Da indicação de marcas ou modelos:**

3.4.1. Não serão exigidas marcas ou modelos específicos para a contratação.

3.5. **Da vedação de utilização de marca ou modelo:**

3.5.1. Não haverá vedação de marca/modelo na presente contratação.

3.6. **Da exigência de carta de solidariedade:**

3.6.1. Não será exigida a apresentação de carta de solidariedade na presente contratação.

3.7. **Da garantia do produto, da manutenção e da assistência técnica:**

Será aplicada ao produto/bem somente a garantia de no mínimo de 60 (sessenta) meses, ou pelo prazo fornecido pelo fabricante, se superior, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

3.7.1 A garantia será prestada com vistas a manter os bens fornecidos em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o Contratante.

3.7.2 A garantia abrange a realização da manutenção corretiva dos bens pelo próprio Contratado, ou, se for o caso, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.

3.7.3 Entende-se por manutenção corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, compreendendo a substituição de peças, a realização de ajustes, reparos e correções necessárias.

3.7.4 As peças que apresentarem vício ou defeito no período de vigência da garantia deverão ser substituídas por outras novas, de primeiro uso, e originais, que apresentem padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento.

3.7.5 Uma vez notificado, o Contratado realizará a reparação ou substituição dos bens que apresentarem vício ou defeito no prazo 10 (dez) dias úteis, contados a partir da data de retirada do produto das dependências da Administração pelo Contratado ou pela assistência técnica autorizada.

3.7.6 O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada do Contratado, aceita pelo Contratante.

3.7.7 Nas hipóteses previstas nos subitens 3.7.8 e 3.7.9 o Contratado deverá disponibilizar produto equivalente, de especificação igual ou superior ao anteriormente fornecido, para utilização em caráter

provisório pelo Contratante, de modo a garantir a continuidade dos trabalhos administrativos durante a execução dos reparos.

3.7.8 Decorrido o prazo para reparos e substituições sem o atendimento da solicitação do Contratante ou a apresentação de justificativas pelo Contratado, fica o Contratante autorizado a contratar fornecedor diverso para executar os reparos, ajustes ou a substituição do bem ou de seus componentes, bem como a exigir do Contratado o reembolso pelos custos respectivos, sem que tal fato acarrete a perda da garantia dos produtos.

3.7.9 O custo referente ao transporte dos produtos cobertos pela garantia será de responsabilidade do Contratado.

3.7.10 A garantia legal ou contratual do objeto tem prazo de vigência próprio e desvinculado do prazo de vigência do contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.

4. MODELO DE EXECUÇÃO DO OBJETO

4.1. **Do prazo de Entrega**

4.1.1. O prazo de entrega do objeto é de até 90 (noventa) dias corridos contados do dia seguinte a confirmação de recebimento da Nota de Empenho, Autorização de Fornecimento ou documento equivalente, em remessa única.

4.1.1.1. A entrega parcelada poderá ser solicitada à Contratante, desde que apresentada justificativas a serem avaliadas, e considerando uma quantidade mínima a ser estabelecida pela Contratante, sendo obrigatório a entrega de todos os componentes do item adquirido. O pagamento poderá ser realizado de acordo com a entrega parcelada.

4.1.2. Devidamente justificado e antes de finalizado o prazo de entrega, o Contratado poderá solicitar prorrogação do prazo da entrega, ficando a cargo da área demandante acolher a solicitação, desde que não haja prejuízo no abastecimento, ressalvadas situações de caso fortuito e força maior, conforme disposto no inciso V, do art. 137, da Lei Federal nº 14.133, de 2021.

4.2. **Do Local e Horário de Entrega**

4.2.1. Os locais de entrega na Polícia Militar, serão determinados no momento da celebração do contrato ou no envio da nota de empenho, de acordo com o endereço listado abaixo:

4.2.1.1. Diretoria de Inteligência - Av. Amazonas, 6.455, bairro Gameleira, Belo Horizonte – MG, entrada pelo 5º Batalhão da Policia Militar, de segunda à sexta no horário de 09h00min (nove horas) às 16h00min (dezesseis horas), exceto às quartas-feiras em que o horário será de 09h00min (nove horas) às 12h00min (doze horas).

5. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

5.1. O fornecedor será selecionado por meio da realização de procedimento na modalidade pregão, conforme art. 28 da Lei Federal nº 14.133, de 2021, sob a forma eletrônica, com adoção do critério de julgamento pelo menor preço , conforme art. 33, da referida Lei Federal, tendo em vista a justificativa apresentada no Estudo Técnico Preliminar (98384615).

5.2. **Dos critérios da aceitabilidade da proposta:**

5.2.1. A proposta terá validade de 90 (noventa) dias corridos contados da data de aceitação.

5.3. **Da Amostra:**

5.3.1. Não será exigida a apresentação de amostras nessa contratação.

5.4. **Da Prova de Conceito (PoC):**

5.4.1. Não será exigida a apresentação de prova de conceito nesta contratação.

5.5. **DA QUALIFICAÇÃO TÉCNICO-OPERACIONAL E TÉCNICO-PROFISSIONAL**

5.5.1. Conforme o Art. 67, inciso VI e § 2º da Lei nº 14.133/21: § 2º Observado o disposto no caput e no § 1º deste artigo, será admitida a exigência de atestados com quantidades mínimas de até 50% (cinquenta

por cento) das parcelas de que trata o referido parágrafo, vedadas limitações de tempo e de locais específicos relativas aos atestados.; a licitante classificada deverá apresentar, para fins de habilitação, 1 (um) ou mais atestados de capacidade técnica que comprove a capacidade de fornecimento dos itens 1, 2 e 3 do Tópico 1 deste Apêndice, OBJETO E CONDIÇÕES GERAIS DA CONTRATAÇÃO. Os atestados de capacidade técnica devem atender os requisitos apresentados neste certame exclusivamente em seu nome, expedidos por pessoa jurídica de direito público ou privado.

_____

Nome Elaborador:

Masp:

_____

Nome Aprovador:

Masp:

Documento assinado eletronicamente por **Anselmo Alves da Rocha**, **1º Tenente**, em 18/12/2024, às 20:49, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **104193839** e o código CRC **6F3FD1C5**.

Referência: Caso responda este Ofício, indicar expressamente o Processo nº 1250.01.0011224/2024-15 SEI nº 104193839

Belo Horizonte, 10 de dezembro de 2024.

Proposta Comercial de Serviço(Lei14133) PMMG/DTS/CSA-TIC LICITAÇÕES Nº 103554823/2024

PROPOSTA COMERCIAL DE SERVIÇO(LEI14133)

ANEXO II DO EDITAL – MODELO DE PROPOSTA COMERCIAL - SERVIÇOS E BENS

PROPOSTA COMERCIAL PARA O PREGÃO ELETRÔNICO Nº 274/2024
(preenchida em papel timbrado da proponente)

DADOS A CONSTAR NA PROPOSTA	PREENCHIMENTO PELO PROPONENTE
Razão Social:	
CNPJ:	
Endereço:	
Telefone:	
Endereço Eletrônico:	
Nome do Representante Legal:	
CPF do Representante Legal:	

	VALOR UNITÁRIO COM ICMS	VALOR UNITÁRIO SEM ICMS	VALOR TOTAL COM ICMS	VALOR TOTAL SEM ICMS
LOTE: Único - _____, conforme especificação técnica do item ____ do Anexo I do Edital de Pregão Eletrônico.	R$	R$	R$	R$
	Quantidade Proposta:			
	Optante pelo Simples Nacional? Não (____) Sim (_____)			
	Marca / Modelo:			
	Prazo de Garantia:			

	VALOR UNITÁRIO COM ICMS	VALOR UNITÁRIO SEM ICMS	VALOR TOTAL COM ICMS	VALOR TOTAL SEM ICMS
LOTE Único : ___ - _____, conforme especificação técnica do item ____ do Anexo I do Edital de Pregão Eletrônico	R$	R$	R$	R$
	Quantidade Proposta:			
	Optante pelo Simples Nacional? Não (_____) Sim (_____)			
	Marca / Modelo:			
	Prazo de Garantia:			

.
.
.

Observações:	
Prazo de Validade da Proposta:	
Prazo de Entrega:	
Local de Entrega:	

Declaro que:

a) serão atendidas todas as condições comerciais estabelecidas no Anexo I – Termo de Referência, deste Edital de Pregão Eletrônico;

b) nos preços propostos encontram-se incluídos todos os tributos, encargos sociais, trabalhistas e financeiros, taxas, seguros e quaisquer outros ônus que porventura possam recair sobre o objeto a ser contratado na presente licitação e que estou de acordo com todas as normas da solicitação de propostas e seus anexos;

c) esta proposta foi elaborada de forma independente;

As informações disponibilizadas neste documento estão sujeitas ao previsto na Lei n.º 13.709, de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD).

Data e local.

Assinatura do Representante Legal da Empresa

Documento assinado eletronicamente por **Isabelle Almeida de Freitas**, **Assessora Jurídica**, em 17/12/2024, às 16:08, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

Documento assinado eletronicamente por **Thiago Vicente de Paula e Silva**, **Major**, em 17/12/2024, às 16:45, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

Documento assinado eletronicamente por **Paulo Gonçalves de Oliveira**, **Major**, em 17/12/2024, às 21:10, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **103554823** e o código CRC **5A6A5421**.

Referência: Processo nº 1250.01.0011224/2024-15 SEI nº 103554823

Belo Horizonte, 10 de dezembro de 2024.

Declarações de Serviço(Lei14133) PMMG/DTS/CSA-TIC LICITAÇÕES Nº 103555371/2024

DECLARAÇÕES DE SERVIÇO(LEI14133)

ANEXO III – MODELOS DE DECLARAÇÃO DE VISTORIA

(PAPEL TIMBRADO DA EMPRESA)

DECLARAÇÃO DE VISTORIA

Em cumprimento à possibilidade facultativa descrita no Edital do **Pregão Eletrônico nº 1250071 274/2024**, declaro que o Sr._____ , CPF _____, devidamente credenciado pela empresa_____, CNPJ: _____, compareceu e vistoriou irrestritamente os locais onde serão executados os serviços objeto da licitação em apreço, e tomou plena ciência das condições locais e das dificuldades existentes, bem como de todas as informações e elementos técnicos, necessários à execução dos serviços a serem licitados.

Por ser verdade, firmamos a presente declaração para que produza seus efeitos de direito.

Data e local.

_____

Assinatura

(PAPEL TIMBRADO DA EMPRESA)

DECLARAÇÃO DE DISPENSA DE VISTORIA

Em cumprimento à possibilidade facultativa descrita no Edital do **Pregão Eletrônico nº 1250071 274/2024** a _____, CNPJ nº _____, com sede à _____, declara, sob as penas da lei, que opta pela não realização de visita técnica, considerando a descrição do serviço contida no Termo de Referência, Anexo do Edital.

Declara e assume inteiramente a responsabilidade e consequências por essa omissão, se compromete a não alegar desconhecimento das condições e grau de dificuldades existentes como justificativa para se eximir das obrigações assumidas ou em favor de eventuais pretensões de acréscimos de preços em decorrência da execução do objeto deste pregão.

Por ser verdade, firmamos a presente declaração para que produza seus efeitos de direito.

Data e local.

_____

Assinatura

Documento assinado eletronicamente por **Isabelle Almeida de Freitas**, **Assessora Jurídica**, em 17/12/2024, às 16:08, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

Documento assinado eletronicamente por **Thiago Vicente de Paula e Silva**, **Major**, em 17/12/2024, às 16:45, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

Documento assinado eletronicamente por **Paulo Gonçalves de Oliveira**, **Major**, em 17/12/2024, às 21:10, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **103555371** e o código CRC **EFD70570**.

Referência: Processo nº 1250.01.0011224/2024-15 SEI nº 103555371

Belo Horizonte, 12 de dezembro de 2024.

Contrato de Serviço(Lei14133) PMMG/DTS/CSA-TIC LICITAÇÕES Nº 103729513/2024

CONTRATO DE SERVIÇO(LEI14133)

ANEXO IV

MODELO DE CONTRATO PARA PRESTAÇÃO DE SERVIÇOS E ENTERGA DE BENS, CRITÉRIO DE JULGAMENTO MENOR VALOR (PREGÃO)

CONTRATO Nº [INSERIR Nº]/[INSERIR ANO], DE PRESTAÇÃO DE SERVIÇOS, QUE ENTRE SI CELEBRAM O ESTADO DE MINAS GERAIS, POR INTERMÉDIO DO [INSERIR NOME DO ÓRGÃO/ENTIDADE] E A EMPRESA [INSERIR NOME DA EMPRESA].

O Estado de Minas Gerais, por intermédio da Polícia Militar de Minas Gerais, representado pelo Centro de Suprimentos e Aquisições de Tecnologia da Informação e Comunicação da PMMG, CSA-TIC/PMMG, com sede na Av. Amazonas, 6.455, bairro Gameleira, Belo Horizonte – MG, CEP 30.510-900, endereço de correio eletrônico: csa-licitacoes@pmmg.mg.gov.br e csatic.pmmg@gmail.com, inscrito no CNPJ sob o nº 16.695.025/0001-97, doravante denominado(a) **CONTRATANTE**, neste ato representado pelo [inserir nome do representante do contratante], inscrito no CPF sob o nº ***.xxx.xxx-**, Resolução de competência nº [inserir nº da resolução de delegação de competência] e [inserir nome do Contratado], endereço de correio eletrônico [inserir e-mail], inscrita no Cadastro Nacional da Pessoa Jurídica – CNPJ – sob o número [inserir nº parcial do CNJP], com sede na [inserir endereço/município], neste ato representada por Sr(a). [inserir nome do representante do contratado], inscrito(a) no CPF nº ***.xxx.xxx-**, doravante denominado **CONTRATADO**, celebram o presente Contrato, decorrente do **Pregão Eletrônico n° 274/2024**, regido pela Lei federal nº 14.133, de 1º de abril de 2021, legislação estadual, e ainda, no que couber, as demais normas específicas aplicáveis ao objeto, ainda que não citadas expressamente.

1. CLÁUSULA PRIMEIRA - OBJETO

1.1. O objeto do presente Contrato é a **contratação/aquisição de Solução de Tecnologia Hiperconvergente,** que deve ser executado conforme condições do Termo de Referência.

1.2. Vinculam esta contratação, independentemente de transcrição:

1.2.1. Termo de Referência;

1.2.2. Aviso de Licitação;

1.2.3. Informações inseridas no Portal de Compras de Minas Gerais;

1.2.4. Proposta comercial do contratado;

1.2.5. Eventuais anexos dos documentos acima.

2. CLÁUSULA SEGUNDA - MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS

2.1. O regime de execução contratual, os modelos de execução e de gestão contratuais, assim como os prazos e condições de entrega e de recebimento do objeto constam no Termo de Referência.

3. CLÁUSULA TERCEIRA - VIGÊNCIA E PRORROGAÇÃO

3.1. O prazo de vigência é de **05 (cinco) anos contados da publicação no Portal Nacional de Contratações Públicas - PNCP, sendo prorrogável, sucessivamente, por até 10 anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.**

3.2. A prorrogação de contrato da parte de serviço contínuo deverá ser promovida mediante celebração de termo aditivo.

3.2.1. A prorrogação de que trata este subitem 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. (art. 107 da Lei nº 14.133/2021).

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

3.4. 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 dos efeitos de aplicação das sanções.

4. CLÁUSULA QUARTA - PREÇO

4.1. O valor da contratação é de R$ [inserir valor] perfazendo o total de R$ [inserir valor].

4.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução contratual, 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.

5. CLÁUSULA QUINTA - DOTAÇÃO ORÇAMENTÁRIA

5.1. As despesas decorrentes desta contratação correrão à conta dos recursos próprios para atender às despesas da mesma natureza, cuja alocação será feita no início de cada exercício financeiro na(s) dotação(ões) orçamentária(s) abaixo indicada(s):

1251 6 181 137 4365 1 3 3 90 39 21 0 9 1, 1251 6 181 137 4365 1 4 4 90 52 7 0 9 1.

Convênio SIAFI nº 9413748.

Nome Convênio: TAC DINT.

Nº Convênio (SIGCON/TransfereGov): 83103951/2024

5.2. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

6. CLÁUSULA SEXTA - PAGAMENTO

6.1. As condições de pagamento estão estabelecidas no Termo de Referência.

7. CLÁUSULA SÉTIMA - DA ALTERAÇÃO DE PREÇOS

7.1. Durante o prazo de vigência, os preços contratados poderão ser reajustados monetariamente com base no IPCA observado o interregno mínimo de 12 meses, contados do orçamento estimado, em 01/11/2024, conforme SEI nº 100822783 e disposto nos arts. 92, §§ 2ºe 3º

da Lei nº 14.133/2021, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

7.2. O direito a que se refere o item 7.1 deverá ser efetivamente exercido mediante pedido formal da contratada até 180 dias após o atingimento do lapso de 12 (doze) meses a que se refere o caput desta cláusula sob pena de preclusão do direito ao seu exercício.

7.3. Os efeitos financeiros retroagem à data do pedido apresentado pela contratada.

7.4. Nos reajustes subsequentes ao primeiro, manter-se-á o marco inicial descrito no item 7.1.

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

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

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

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

7.8. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório.

8. CLÁUSULA OITAVA - OBRIGAÇÕES DA CONTRATANTE E DO CONTRATADO

8.1. As obrigações técnicas relativas à execução do objeto (descrição, funcionamento e aplicação) são descritas no Termo de Referência.

9. CLÁUSULA NONA - GARANTIA DE EXECUÇÃO

9.1. Não haverá exigência de garantia contratual da execução.

10. CLÁUSULA DÉCIMA - SENÇÕES ADMINISTRATIVAS

10.1. As sanções administrativas incidentes à inexecução do objeto são descritas no Termo de Referência.

11. CLÁUSULA DÉCIMA PRIMEIRA - DA EXTINÇÃO

11.1. O contrato será extinto quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes.

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

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

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

11.4. O contrato poderá ser extinto em decorrência do não cumprimento das obrigações relativas à reserva de cargos prevista em lei, bem como em outras normas específicas, para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, antes de cumpridas as

obrigações nele estipuladas, ou antes do prazo nele fixado, e demais motivos previstos no artigo 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

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

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

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

11.6. O termo de extinção será precedido de relatório indicativo dos seguintes aspectos, conforme o caso:

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

11.6.2. Relação dos pagamentos já efetuados e ainda devidos;

11.6.3. Indenizações e multas.

11.7. As partes entregarão, no momento da extinção, a documentação e eventual material de propriedade da outra parte, acaso em seu poder.

11.8. No procedimento que visar à extinção do vínculo contratual, precedida de autorização escrita e fundamentada da autoridade competente, será assegurado o devido processo legal, o contraditório e a ampla defesa, sem prejuízo da possibilidade de a CONTRATANTE adotar, motivadamente, providências acauteladoras.

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

12. CLÁUSULA DÉCIMA SEGUNDA - DA PROTEÇÃO DE DADOS PESSOAIS

12.1. As PARTES, por si e por seus colaboradores, obrigam-se a atuar no presente contrato em conformidade com a legislação vigente sobre Proteção de Dados Pessoais e as determinações de órgão reguladores e/ou fiscalizadores sobre a matéria, em especial, a Lei Federal nº 13.709/2018.

12.2. No presente contrato, a CONTRATANTE assume o papel de controlador e o CONTRATADO assume o papel de operador conforme artigo 5º, VI e VII da Lei nº 13.709/2018.

12.3. O CONTRATADO deverá guardar sigilo sobre os dados pessoais compartilhados pela CONTRATANTE e só poderá fazer uso dos dados exclusivamente para fins de cumprimento do objeto deste contrato, sendo-lhe vedado, a qualquer tempo, o compartilhamento desses dados sem a expressa autorização da CONTRATANTE, ou o tratamento dos dados de forma incompatível com as finalidades e prazos acordados.

12.4. As PARTES deverão notificar uma à outra, por meio eletrônico, em até 5 (cinco) dias úteis, sobre qualquer incidente detectado no âmbito de suas atividades, relativo a operações de tratamento de dados pessoais.

12.5. As PARTES se comprometem a adotar as medidas de segurança administrativas, tecnológicas, técnicas e operacionais necessárias a resguardar os dados pessoais que lhe serão confiados, levando em conta as diretrizes de órgãos reguladores, padrões técnicos e boas práticas existentes.

12.6. A CONTRATANTE terá o direito de acompanhar, monitorar, auditar e fiscalizar a conformidade do CONTRATADO, diante das obrigações de operador, para a proteção de dados pessoais referentes à execução deste contrato.

12.7. As PARTES ficam obrigadas a indicar encarregado pela proteção de dados pessoais, ou preposto, para comunicação sobre os assuntos pertinentes à Lei nº 13.709/2018, suas alterações e regulamentações posteriores, quando necessário.

12.8. As PARTES darão conhecimento formal a seus empregados e colaboradores das obrigações e condições acordadas nesta cláusula. As diretrizes aqui estipuladas deverão ser aplicadas a toda e qualquer atividade que envolva a presente contratação.

13. CLÁUSULA DÉCIMA TERCEIRA - ALTERAÇÕES

13.1. O presente contrato poderá ser alterado nos casos previstos pelo art. 124 de Lei n.º 14.133/2021, desde que devidamente motivado e autorizado pela autoridade competente.

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

13.1.2. 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).

13.1.3. 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 - DOS CASOS OMISSOS

14.1. Os casos omissos serão decididos pela CONTRATANTE, segundo as disposições contidas na Lei nº 14.133/2021, Decreto-Lei nº 4.657/1942 (Lei de Introdução às Normas do Direito Brasileiro) e demais normas relativas a licitações e contratos administrativos e, subsidiariamente, a Lei nº 8.078/1990 - Código de Defesa do Consumidor, ainda normas e princípios gerais dos contratos.

15. CLÁUSULA DÉCIMA QUINTA - PUBLICAÇÃO

15.1. Este contrato será publicado no Portal Nacional de Contratações Públicas (PNCP).

15.1.1. O Portal de Compras será integrado ao PNCP para fins de cumprimento do art. 94 da Lei 14.133, de 2021.

16. CLÁUSULA DÉCIMA SEXTA - FORO

16.1. As partes elegem o foro da Comarca de Belo Horizonte, Minas Gerais, para dirimir quaisquer dúvidas ou litígios decorrentes deste Contrato.

E, por estarem ajustadas, firmam as partes este instrumento assinado eletronicamente.

Documento assinado eletronicamente por **Isabelle Almeida de Freitas**, **Assessora Jurídica**, em 17/12/2024, às 16:08, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

Documento assinado eletronicamente por **Thiago Vicente de Paula e Silva**, **Major**, em 17/12/2024, às 16:45, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

Documento assinado eletronicamente por **Paulo Gonçalves de Oliveira**, **Major**, em 17/12/2024, às 21:10, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **103729513** e o código CRC **61E6C61D**.

Referência: Processo nº 1250.01.0011224/2024-15 SEI nº 103729513

TERMO ADITIVO DE CONVÊNIO

PMMG 3ºBPM x Município de Couto Magalhães de Minas MG - Primeiro Termo Aditivo do Convênio 06/2021. Objeto: Alterar o item 4.1 da cláusula Quarta (Do valor), passando a totalizar o valor de R$228.856,97 (duzentos e vinte e oito mil, oitocentos e cinquenta e seis reais e noventa e sete centavos), bem como a cláusula Sexta (Da Vigência), ficando prorrogado a data do convênio até 31/03/2025 e estabelecer novo plano de trabalho para o período aditado.

2 cm -17 2024585 - 1

HOMOLOGAÇÃO DE PREGÃO RP

HOMOLOGAÇÃO DE PREGÃO RP PMMG-DS-CSC/SAÚDE - Pregão Eletrônico nº 219/2024 - SEI 1250.01.0013550/2024-69 Objeto: Registro de Preços para aquisição de equipamentos e mobiliários odontológicos, médicos, cirúrgicos, fisioterápicos e laboratoriais, sob demanda, futura e eventual, conforme especificações, exigências e quantidades estabelecidas no Edital e Anexos. A íntegra do termo de conclusão disponível no site www.compras.mg.gov.br.

2 cm -17 2024532 - 1

HOMOLOGAÇÃO DE PREGÃO

PMMG - DS - CSC/SAÚDE - Pregão Eletrônico nº 1451978 000027/2024 - SEJUSP - Processo SEI nº 1250.01.0014059/2024-03. Objeto: contratação de empresa especializada para a confecção, montagem e instalação de mobiliários sob medida/planejados, incluindo material e mão de obra, para a clínica de fisioterapia da APM, conforme especificações, exigências e quantidades estabelecidas no Edital e seus anexos. Disponível no site www.compras.mg.gov.br e Sistema SEI/MG processo nº 1250.01.0014059/2024-03.

2 cm -17 2024533 - 1

EXTRATO TERMO ENCERRAMENTO
CONTRATO Nº 9346150/2022 – 18º RPM

Extrato do Termo de Encerramento do Contrato nº 9346150/2022 de Serviço, firmado entre o Estado de Minas Gerais por meio da PMMG e o fornecedor 34.683.835/0001-05 – Recon Construtora Ltda, Processo nº 1259973 058/2022, Pregão eletrônico. Objeto: Contratação de empresa de prestação de serviços de reforma, reparo e restauração do telhado, com engradamento de madeira, e reparo nas lajes e paredes danificadas pela infiltração e substituição das calhas, rufos e pintura interna e externa da edificação da seção de saúde do 12º batalhão de polícia militar, conforme anexo 01 - termo de referência. Encerramento do contrato a partir de 12/12/2024.

EXTRATO TERMO ENCERRAMENTO
CONTRATO Nº 9394366/2023 – 18º RPM

Extrato do Termo de Encerramento do Contrato nº 9394366/2023 de Serviço, firmado entre o Estado De Minas Gerais por meio da PMMG e o fornecedor 19.499.671/0001-77 – Ms Serviços De Manutenção Ltda, Processo nº 1259973 047/2023, Pregão eletrônico.Objeto: Contratação de empresa especializada para realizar o serviço de manutenção, reparo, conservação e adaptação em equipamentos e instrumentos odontológicos das Seções de Assistência à Saúde - (SAS), na 18ª RPM (Poços de Caldas), 12º BPM (Passos), 43º BPM (São Sebastião do Paraíso) e 64º BPM (Alfenas), com fornecimento de peças para substituição se necessário, conforme especificações, exigências e quantidades estabelecidas neste documento. Encerramento do contrato a partir de 12/12/2024.

6 cm -17 2024559 - 1

AVISO DE LICITAÇÃO

PMMG-CSA-TIC: Pregão Eletrônico 1250071 274/2024. Objeto: Contratação/aquisição de Solução de Tecnologia Hiperconvergente. As propostas comerciais deverão ser enviadas através do site www.compras.mg.gov.br, até o dia 07/01/2025, às 08h55. A abertura da seção de lances será a partir das 09h. da mesma data. Informações fone (31) 2123-1018. Edital disponível em www.compras.mg.gov.br e https://portal.policiamilitar.mg.gov.br/portal-pm/licitacao.action e Portal Nacional de Compras.

2 cm -17 2024588 - 1

TERMO DE COOPERAÇÃO TÉCNICA

PMMG-19ª Cia PM Ind x Prefeitura Municipal de Igaratinga/MG. Termo de cooperação técnica n 01/2024. Cessão gratuita pela Prefeitura da infraestrutura da antena instalada em imóvel de propriedade da mencionada partícipe para que seja instalada uma estação repetidora com a respectiva antena, localizada na Rua Monte Calvário, defronte o nr 23, bairro Bom Pastor, município de Igaratinga. Vigência: indeterminada.

2 cm -17 2024618 - 1

EXTRATO TERMO ADITIVO

PMMG 7º BPM x Prefeitura de Pompéu/MG. 1º Termo aditivo Convênio 06/2024. Objeto: majoração de valores do convênio, devido ao acréscimo de aquisição de combustível e lubrificantes para suprir a demanda operacional não prevista no convênio original. Valor total do convênio passa a R$120.459,74. Vigência 01/12/24 a 31/12/24.

2 cm -17 2024622 - 1

TERMO DE CESSÃO DE USO

PMMG – 19ª Cia PM Ind x Prefeitura Municipal de Papagaios/MG. Cessão de Uso nº 01/2024. Objeto: empréstimo gratuito de 01 imóvel situado na Rua Hélio Filgueiras, nº 155, bairro Centro, município de Papagaios/MG, com área total de 675 m2 e área construída de 184,23 m2. Vigência:12/04/2024 a 12/041/2049.

2 cm -17 2024604 - 1

HOMOLOGAÇÃO DE PREGÃO

PMMG-2RPM. Pregão Eletrônico – Processo de Compra: 1259966 74/2024. Objeto: contratação de empresa especializada de engenharia/arquiteturа destinada a executar a reforma dos vestiários na sede do 48º Batalhão de Polícia Militar, em Ibiritê/MG. Lote 01 CNPJ 33.385.398/0001-80 - CONSTRUIR ENGENHARIA LTDA, valor R$ 121.431,20. A integra da Ata e Termo de Conclusão do Pregão, disponível no site: www.compras.mg.gov.br

2 cm -17 2024633 - 1

EXTRATO DE CONTRATO – ERRATA

Onde se lê:
Extrato do Contrato 9445776, firmado entre o ESTADO DE MINAS GERAIS por meio da PMMG/14RPM e o fornecedor ABADE & CAPELLI INDUSTRIA E COMERCIO DE MOVEIS LTDA, CNPJ 20.323.529/0001-53, Processo de Compras 1259969 00061/2024; Objeto: Aquisição de itens de mobiliário para a nova sede da 14ª Região de Polícia Militar, sendo bancos para assento. Valor total estimado da contratação: R$2.091,25(dois mil e noventa e um reais e vinte e cinco centavos). Vigência até 13/12/2025.
Leia-se:
Extrato do Contrato 9445776, firmado entre o ESTADO DE MINAS GERAIS por meio da PMMG/14RPM e o fornecedor ABADE & CAPELLI INDUSTRIA E COMERCIO DE MOVEIS LTDA, CNPJ 20.323.529/0001-53, Processo de Compras 1259969 00061/2024; Objeto: Aquisição de itens de mobiliário para a nova sede da 14ª Região de Polícia Militar, sendo bancos para assento. Valor total estimado da contratação: R$2.091,25(dois mil e noventa e um reais e vinte e cinco centavos). Vigência até 18/06/2025.

4 cm -17 2024708 - 1

EXTRATO DE CONTRATO – ERRATA

Onde se lê:
Extrato do Contrato 9445674, firmado entre o ESTADO DE MINAS GERAIS por meio da PMMG/14RPM e o fornecedor UFFÍCIO INDÚSTRIA E COMÉRCIO DE MÓVEIS LTDA, CNPJ 04.443.182/0001-26, Processo de Compras 1259969 00061/2024; Objeto: Aquisição de itens de mobiliário para a nova sede da 14ª Região de Polícia Militar, sendo estação de trabalho e cadeira para escritório. Valor total estimado da contratação: R$29.421,00(vinte e nove mil, quatrocentos e vinte e um reais). Vigência até 13/12/2025.
Leia-se:
Extrato do Contrato 9445674, firmado entre o ESTADO DE MINAS GERAIS por meio da PMMG/14RPM e o fornecedor UFFÍCIO INDÚSTRIA E COMÉRCIO DE MÓVEIS LTDA, CNPJ 04.443.182/0001-26, Processo de Compras 1259969 00061/2024; Objeto: Aquisição de itens de mobiliário para a nova sede da 14ª Região de Polícia Militar, sendo estação de trabalho e cadeira para escritório. Valor total estimado da contratação: R$29.421,00(vinte e nove mil, quatrocentos e vinte e um reais). Vigência até 18/06/2025.

4 cm -17 2024706 - 1

EXTRATO DE CONVÊNIO Nº 02/2025 – SERRANIA

PMMG 64º BPM X PREFEITURA DE SERRANIA Convênio nº 02/2025 - Objeto: cooperação mútua, visando aperfeiçoar o policiamento ostensivo e a preservação da ordem pública no município - Vigência: 01/01/2025 a 31/12/2025

1 cm -17 2024693 - 1

EXTRATO DE TERMO DE COMODATO

PMMG -28º BPM x COSEP RURAL DE UNAI/MG. Termo de Comodato nº 07/2024; Objeto: empréstimo gratuito de 01 caminhonete marca TOYOTA, modelo HILUX CDSR A4FD, placa TDF6168, CHASSI: 8AJKA3CD4R3138298 cor preta, 4X4, diesel, ano/modelo 2024, nova, caracterizada. Vigência 17/12/2024 a 17/12/2029.

2 cm -17 2024754 - 1

EXTRATO DE CONVÊNIO Nº 03/2025 –
CONCEIÇÃO DA APARECIDA

PMMG 64º BPM X PREFEITURA DE CONCEIÇÃO DA APARECIDA Convênio nº 03/2025 - Objeto: cooperação mútua, visando aperfeiçoar o policiamento ostensivo e a preservação da ordem pública no município - Vigência: 01/01/2025 a 31/12/2025

2 cm -17 2024805 - 1

PUBLICAÇÃO TERMO ADITIVO AO
CONTRATO 009443842/2024 PROCESSO 1451978
000041/2024 COTAÇÃO ELETRONICA

Publicação do Termo aditivo ao Contrato Nr 009443842/2024 que entre si celebram o Estado de Minas Gerais por meio do Comando de Policiamento Especializado e a empresa WM Portas Empreendimentos em móveis Planejados Ltda – EPP. Objeto: acréscimo do serviço personalizados de MDF com tamanhos e formatos personalizados e acessórios, para fabricação e montagem de armários e demais estruturas de marcenaria na sede da Companhia de Recobrimento e Eventos do CPE conforme as especificações e quantidades apresentadas em nova proposta complementar, tendo como parâmetro contrato firmado e documentos complementares que deve ser executado conforme condições estabelecidas previamente. A conforme especificações e quantitativos estabelecidos no termo de Referência e anexo do Edital. Valor do aditivo: R$8.956,48 (oito mil novecentos e cinquenta e seis mil reais e quarenta e oito centavos). Validade do contrato: 31/12/2024

4 cm -17 2024900 - 1

EXTRATO DE CONTRATO

PMMG-2RPM X 33.385.398/0001-80- CONSTRUIR ENGENHARIA LTDA, Pregão 1259966 74/2024 contrato nº 9446085. Objeto: contratação de empresa especializada de engenharia/arquiteturа destinada a executar a reformados vestiários na sede do 48º BPM em Ibiritê, para atender requisito previsto na Lei 14.133/2021 nas licitações da 2ª RPM. Valor R$ 121.431,20.

2 cm -17 2024954 - 1

EXTRATO DE CONTRATO

PMMG-CSA-TIC- Contrato nº 9.446.153/2024 - Processo de compra: 1250071 280/2024, celebrado entre a PMMG-CSA-TIC, CNPJ 16.695.025/0001-97 e a empresa REPREMIG REPRESENTAÇÃO E COMÉRCIO DE MINAS GERAIS LTDA, CNPJ 65.149.197/0002-51. Objeto: Aquisição de 03 soluções básicas de video wall e monitores para a ampliação da solução básica, incluindo instalação, configuração e acessórios necessários, conforme especificações e quantitativos estabelecidos no Edital do Pregão nº333/2023. Valor do Contrato: R$ 27.000,00. Vigência 12 meses,meses, a partir dessa publicação.

3 cm -17 2024958 - 1

AVISO DE LICITAÇÃO

PMMG - EM/14º RPM. Cotação Eletrônica; Processo de Compras 1259969 00084/2024; UE: 1250086; Objeto: contratação de Empresa especializada em instalação de equipamentos de ar condicionado com o fornecimento de todo material necessário, instalação com mão de obra e equipamentos necessários ao perfeito funcionamento. Data de início para recebimento das propostas: entre 17/12/2024, 16:33(horário de Brasília) até 23/12/2024, 07:59 (horário de Brasília). Data/hora de abertura e fechamento da sessão de lances da cotação eletrônica: entre 08h00min até às 14h00min do dia 23/12/2024. ID contratação PNCP: 16695025000197-1-001437/2024.

3 cm -17 2024961 - 1

EXTRATO DE CONTRATO

PMMG-CSA-TIC- Contrato nº 9.445.963/2024 - processo de compra 1250071 273/2024, celebrado entre a PMMG-CSA-TIC, CNPJ 16.695.025/0001-97 e a empresa DRIVE A INFORMÁTICA LTDA., CNPJ 00.677.870/0001-08. Objeto: Computador Avançados - Workstation. Valor do Contrato: R$ 13.943,00. Vigência 01 (um) ano contado a partir do primeiro dia útil subsequente à assinatura do contrato, na forma do artigo, 105 da Lei nº 14.133, de 2021.

2 cm -17 2024965 - 1

TERMO ADITIVO

PMMG/DF – 06 TA Convênio 13/2022. PARTES: Estado de Minas Gerais por intermédio da Polícia Militar de Minas Gerais e a Prefeitura de Uberaba/MG. OBJETO: Alterar vigência e estabelecer novo plano de trabalho. VALOR: R$912.000,00. VIGÊNCIA: 31/12/2025. ASSINATURA: 17/12/2024.

2 cm -17 2024968 - 1

TERMO ADITIVO

PMMG/DF – 02 TA Convênio 162/2022. PARTES: Estado de Minas Gerais por intermédio da Polícia Militar de Minas Gerais e a Prefeitura de Igarapé/MG. OBJETO: Alterar vigência acrescentar valor e estabelecer novo plano de trabalho. VALOR: R$1.124.405,29. VIGÊNCIA: 31/12/2027. ASSINATURA: 17/12/2024.

2 cm -17 2024964 - 1

Instituto de Previdência dos Servidores Militares do Estado de Minas Gerais - IPSM

RESUMO DE HABILITADOS

O Cel PM QOR André Luís Dias Machado, Diretor de Saúde do IPSM, (delegação conforme disposto no art. 36º, do Decreto Estadual nº 48.064, de 16/10/2020 e Portaria 941/2021- DG/IPSM de 04/02/2021), cumprindo o disposto no subitem 11.4 do Edital de Credenciamento nº 06/2023, divulga os interessados HABILITADOS em credenciar-se no Sistema de Saúde da PMM-CBMMG-IPSM no âmbito da região da Polícia Militar/MG. Data: 17/12/2024

8ª RPM – Governador Valadares

Município	Interessado	Categoria
Itabirinha	Bicalho Odontologia Ltda	Clínica Odontológica

9ª RPM – Uberlândia

Município	Interessado	Categoria
Uberlândia	Santos & Catani Serviços Médicos	Clínica Médica
Ituiutaba	Vilela Odontologia Ltda	Clínica Odontológica
	Clínica Médica e Diagnostico de Imagem Ituiutaba Ltda	Clínica Médica

12ª RPM – Ipatinga

Município	Interessado	Categoria
Iapu	Beatriz Vieira Mafra	Laboratório Clínico

18ª RPM – Poços de Caldas

Município	Interessado	Categoria
Poços de Caldas	Menossi Serviços Médicos Sociedade Simples Ltda	Clínica Médica
Alfenas	Elaborare Clínica de Psicologia Ltda	Serviço de Psicologia

RESUMO DE NÃO HABILITADOS

O Cel PM QOR André Luis Dias Machado, Diretor de Saúde do IPSM, (delegação conforme disposto no art. 36º, do Decreto Estadual nº 48.064, de 16/10/2020 e Portaria 941/2021- DG/IPSM de 04/02/2021), cumprindo o disposto nos subitens 8.3.1; 9.2.1 e 11.4 do Edital de Credenciamento nº 06/2023, divulga os interessados NÃO HABILITADOS em credenciar-se no Sistema de Saúde da PMMG-CBMMG-IPSM no âmbito da região da Polícia Militar/MG.
Data: 17/12/2024
RMBH

Município	Interessado	Itens Pendentes Anexo II
Belo Horizonte	Clínica de Fisioterapia e Longevidade Renato Caran Ltda	VII, IX
	Marcos Correia Lima	IV,VI,XIV,XVI

9ª RPM- Uberlândia

Município	Interessado	Itens Pendentes Anexo II
Uberlândia	Uberlândia Odonto Center Uoc Ltda	IV, XIV

18ª RPM- Poços de Caldas

Município	Interessado	Itens Pendentes Anexo II
Poços de Caldas	Centro Médico e Laboratorial São Camilo Ltda	IV,IX, XVII

Nos termos estabelecidos no subitem 11.7 do Edital de Credenciamento nº 06/2023, fica concedido o prazo de 05 (cinco) dias úteis, contados do primeiro dia útil subsequente a esta divulgação, para a apresentação de recurso pelos interessados em relação à avaliação da documentação entregue no ato de inscrição.

RESUMO DE NÃO HABILITADO

O Cel PM QOR André Luis Dias Machado, Diretor de Saúde do IPSM, (delegação conforme disposto no art. 36º, do Decreto Estadual nº 48.064, de 16/10/2020 e Portaria 941/2021- DG/IPSM de 04/02/2021), cumprindo os dispostos nos subitens 9.2.1 e 11.4 do Edital nº 06/2023, divulga o interessado NÃO HABILITADO em credenciar-se no Sistema de Saúde da PMMG-CBMMG-IPSM no âmbito da região da Polícia Militar/MG, por não apresentar os documentos do Anexo II. Data: 17/12/2024
8ª RPM – Governador Valadares

Município	Interessado
Itanhomi	Peres Implantart Odontologia Especializada Ltda

Nos termos estabelecidos no subitem 11.7 do Edital de Credenciamento nº 06/2023, fica concedido o prazo de 05 (cinco) dias úteis, contados do primeiro dia útil subsequente a esta divulgação, para a apresentação de recurso pelos interessados em relação à avaliação da documentação entregue no ato de inscrição.

28 cm -17 2024919 - 1

Polícia Civil do Estado de Minas Gerais

EXTRATOS DE CONTRATOS
EXTRATO DO I TERMO ADITIVO AO
CONTRATO Nº 9439873/2024
PROCESSO DE COMPRAS Nº 1511189 000243/2024
PROCESSO ELETRÔNICO Nº 1510.01.0180301/2024-84

Partes: EMG/Polícia Civil e a Pessoa Jurídica ECCOPOWER SISTEMAS DE ENERGIA IMPORTACAO, EXPORTACAO LTDA. Objeto: acréscimo em 25% do item SIAD 001913689, para aquisição de mais 10 (dez) unidades de nobreaks, por meio de recursos provenientes de emenda parlamentar de indicação nº 141134. Valor do termo aditivo: R$ 3.000,00 (três mil reais); o valor global do contrato passará de R$ 12.000,00 (doze mil reais) para R$ 15.000,00 (quinze mil reais). Dotação Orçamentária: 1511.06.181.032.1007.0001.4.4.90 .52.07.1.10.8. Foro: B.Hte/MG. Assinatura: 17/12/2024. Signatários: Andrea Mendes de Souza Abood (P/Contratante) e Vitor Pedro Alves (P/ Contratada).

EXTRATO DO II TERMO ADITIVO DO
CONTRATO Nº 9370814/2022
PROCESSO DE COMPRAS Nº 1511189 000232/2022
PROCESSO ELETRÔNICO Nº 1510.01.0182474/2022-07

Partes: EMG/Polícia Civil e a Pessoa Jurídica APOLO REFRIGERACAO LTDA. Do objeto: a prorrogação do prazo de vigência do contrato número 9370814/2022, prestação de serviços de manutenção preventiva, preditiva, corretiva e implantação do PMOC (Programa de Manutenção, Operação e Controle), balanceamento de insuflamento de ar e correções no isolamento termo-acústico nos Sistemas de Refrigeração, com substituição de peças, por 12 (doze) meses e, o reajuste do valor global do contrato no percentual de 4,42% considerando IPCA de setembro/2024 (99142051). Valor total: R$ 54.298,36 (cinquenta e quatro mil duzentos e noventa e oito reais e trinta e seis centavos). Vigência: 12 (doze) meses, com início em 28/12/2024 e término em 27/12/2025. Dotação Orçamentária: 1511.06.422.036.40 65.0001.3.3.90.39.21.0.10.1. Foro: B.Hte/MG. Assinatura: 17/12/2024. Signatários: Andrea Mendes de Souza Abood (P/Contratante) e Marcos Aurélio Pinheiro (P/ Contratada).

8 cm -17 2025012 - 1

EXTRATOS DE CONTRATOS
HOMOLOGAÇÃO
PREGÃO ELETRÔNICO Nº 1451977 046/2024

SEI: 1510.01.0201557/2024-24. Objeto: Contratação de serviços de fornecimento de Subscrição de licença do software de análise investigativa i2 Analyst's Notebook via TDCO nº 11/2022
Lote 01 Empresa Vencedora OWL 4TECH LTDA – Valor R$ 239.940,00

Belo Horizonte, 17 de dezembro de 2024.
Antônio Cipriano das Neves Silva
Diretor de Aquisições

PREGÃO ELETRÔNICO Nº 1451977 048/2024

SEI: 1510.01.0211797/2024-91.Objeto: Contratação da prestação de serviços de fornecimento de licenças dos Softwares Qliksense Analyser e Professional para a Polícia Civil de Minas Gerais.
Lote 01 Empresa Vencedora INTELIGÊNCIA DE NEGÓCIOS, SISTEMAS E INFORMÁTICA LTDA Valor R$ 248.021,00.

Belo Horizonte, 17 de dezembro de 2024.
Antônio Cipriano das Neves Silva
Diretor de Aquisições

PREGÃO ELETRÔNICO Nº 1451977 047/2024

SEI: 1510.01.0183686/2024-63.Objeto: Contratação de serviços de contratação de serviços de renovação de Suporte Técnico e Atualização dos Softwares QLIKSENSE ANALYSER, PROFESSIONAL E NPRINTING.
Lote 01 Empresa Vencedora INTELIGÊNCIA DE NEGÓCIOS, SISTEMAS E INFORMÁTICA LTDA Valor R$ 97.000,00(noventa e sete mil reais)

Belo Horizonte, 17 de dezembro de 2024.
Antônio Cipriano das Neves Silva
Diretor de Aquisições

PREGÃO ELETRÔNICO Nº 1451977 055/2024

SEI: 1510.01.0194046/2024-91.Objeto: Compra de materiais para acondicionamento e custódia de vestigios criminais
Lote 01 Fracassado
Lote 02 Empresa Vencedora: FOCOS COMERCIAL LTDA
Valor R$ 12.000,00(Doze mil reais)
Lote 03 Empresa Vencedora: FOCOS COMERCIAL LTDA
Valor R$18.720,00 (Dezoito mil, setecentos e vinte reais)

Belo Horizonte, 17 de dezembro de 2024.
Antônio Cipriano das Neves Silva
Diretor de Aquisições

PREGÃO ELETRÔNICO Nº 1511189 268/2024

SEI: 1510.01.0208854/2024-12.Objeto: Contratação da prestação de serviços de fornecimento de subscrição de licenças dos Softwares Qliksense Analyser e Professional para a Polícia Civil de Minas Gerais
Lote 01 Deserto

Belo Horizonte, 17 de dezembro de 2024.
Antônio Cipriano das Neves Silva
Diretor de Aquisições

PREGÃO ELETRÔNICO Nº 1511189 253/2024

SEI: 1510.01.0193311/2024-51.Objeto: Contratação de serviços de Contratação do Software I2 ANALYST´S NOTEBOOK para a Polícia Civil de Minas Gerais
Lote 01 Empresa Vencedora: OWL 4TECH LTDA.
Valor homologado: R$ 79.980,00(setenta e nove mil novecentos e oitenta reais)

Belo Horizonte, 17 de dezembro de 2024.
Antônio Cipriano das Neves Silva
Diretor de Aquisições

EXTRATO DO TERMO DE CONTRATO Nº 9445992/2024

PROCESSO DE COMPRAS Nº 1451977 63/2024. PROCESSO ELETRÔNICO Nº 1510.01.0276269/2024-12.Partes: EMG/Polícia Civil e a Pessoa Jurídica INSPECT INTELIGENCIA E TECNOLOGIA LTDA. Do objeto: aquisição de solução tecnológica para reconhecimento facial e análise de imagens, Software Clearview Professional para a Superintendência de Informações e Inteligência Policial/SIIP da Polícia Civil de Minas Gerais. Valor total: R$ 428.400,00 (quatrocentos e vinte e oito mil e quatrocentos reais). Vigência: 36 (trinta e seis) meses contado a partir do primeiro dia útil subsequente à assinatura do contrato. Dotação Orçamentária: 4691.06.123.134.2071.0001.4.4.9 0.40.06.0.57.1. Foro: B.Hte/MG. Assinatura: 16/12/2024. Signatários: Andrea Mendes de Souza Abood (P/Contratante) e Luiz Henrique de Souza Borges (P/ Contratada).

17 cm -17 2024777 - 1