

EDITAL

**Republicado em virtude de alteração de data de abertura*
UASG - 926181

PREGÃO ELETRÔNICO Nº 90005/2025 - SRP **Processo Administrativo nº 0217/2025**

Torna-se público, para conhecimento dos interessados, que a Assembleia Legislativa do Tocantins, através do Pregoeiro designado por meio da Portaria nº 057/2024 - DG de 11/01/2024, sediada no Palácio João D'Abreu, Praça dos Girassóis, Centro, Palmas – TO, realizará licitação, na modalidade PREGÃO, na forma ELETRÔNICA, modo ABERTO, com critério de julgamento MENOR PREÇO, utilizando-se o Registro de Preços, nos termos da Lei nº 14.133, de 1º de abril de 2021 e alterações posteriores, do Decreto Administrativo nº 552/2024 de 05/06/2024, bem como as condições estabelecidas neste Edital e seus Anexos.

Data da sessão: 26/06/2025

Horário: 08h30 min. Horário de Brasília – DF.

Local: Sistema de Compras do Governo Federal (www.gov.br/compras).

Toda e qualquer alteração que possivelmente ocorrer neste Edital, tais como errata, adendo, suspensão ou revogação, deverá ser consultada pelos pretensos licitantes no endereço eletrônico do Sistema de Compras do Governo Federal (www.gov.br/compras), bem como no site da Assembleia Legislativa do Tocantins: www.al.to.leg.br “licitação”.

A Administração não se responsabilizará caso o pretenso licitante não acesse o endereço eletrônico informado ou não visualize a alteração no Site supracitado, consequentemente desconhecendo o teor dos Avisos publicados.

1. DO OBJETO

1.1. O objeto da presente licitação é a escolha da proposta mais vantajosa para Registro de Preços para a futura contratação de empresa especializada na prestação de serviços de CLOUD COMPUTING de infraestrutura TIC, baseado na plataforma IaaS (Infraestrutura como serviço), para atendimento às necessidades da Assembleia Legislativa do Tocantins, conforme quantidades e condições estabelecidas neste Edital e seus anexos.

1.2. A licitação será em grupo único conforme tabela constante do Termo de Referência.

1.3. O critério de julgamento adotado será o menor preço global, observadas as condições contidas neste Edital e seus Anexos.

1.4. A descrição detalhada dos itens que compõem o grupo e seus respectivos quantitativos, encontram-se pormenorizadas em tópico específico do Termo de Referência, Anexo I deste Edital.

3. DA PARTICIPAÇÃO NO PREGÃO

3.1. Poderão participar deste certame os interessados cujo ramo de atividade seja compatível com o objeto da licitação e que estiverem previamente credenciados no Sistema de

Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras).

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

3.3. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

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

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

3.6. Não será concedido o tratamento favorecido para as ME/EPP previsto nos arts. 42 a 49 da Lei Complementar nº 123/2006 e suas alterações posteriores, quando o objeto da licitação se enquadrar ao disposto no inciso I, § 1º, art. 4º, da Lei nº 14.133/2021.

3.7. Não poderão disputar esta licitação:

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

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

3.7.3. sociedades cooperativas;

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

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

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

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

3.7.8. 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;

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

3.7.10. 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;

3.7.11. pessoas jurídicas reunidas em consórcio;

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

3.8. Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público do órgão ou entidade contratante, devendo ser observadas as situações que possam

configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme § 1º do art. 9º da Lei nº 14.133, de 2021.

3.9. O impedimento de que trata o item 3.7.7 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.

3.10. A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem os itens 3.7.5 e 3.7.6 poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.

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

3.12. O disposto nos itens 3.7.5 e 3.7.6 não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.

3.13. A vedação de que trata o item 3.8 estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

4. DO ORÇAMENTO ESTIMADO

4.1. O orçamento estimado para a presente contratação é de R\$ 2.702.040,00 (dois milhões, setecentos e dois mil e quarenta reais).

5. DA APRESENTAÇÃO DA PROPOSTA

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

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

5.3. Caso a fase de habilitação anteceda as fases de apresentação de propostas e lances, os licitantes encaminharão, na forma e no prazo estabelecidos no item anterior, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto, observado o disposto neste Edital.

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

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

5.4.2. não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7º, XXXIII, da Constituição;

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

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

- 5.5. O licitante organizado em cooperativa, caso permitida a sua participação, deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 16 da Lei nº 14.133, de 2021.
- 5.6. O licitante deverá declarar em campo próprio do sistema se o produto ou serviço ofertado é manufaturado nacional beneficiado por um dos critérios de margem de preferência indicados no Termo de Referência, quando for o caso, para usufruir do benefício.
- 5.7. O fornecedor enquadrado como microempresa, empresa de pequeno porte ou sociedade cooperativa deverá declarar, ainda, quando a licitação permitir o tratamento diferenciado, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 3º da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021.
- 5.7.1 No item exclusivo para participação de microempresas e empresas de pequeno porte, quando houver, a assinalação do campo “não” impedirá o prosseguimento no certame, para aquele item;
- 5.7.2 Nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte ou sociedade cooperativa.
- 5.8. A falsidade da declaração de que trata os itens 5.4 ou 5.7 sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.
- 5.9. Os licitantes poderão retirar ou substituir a proposta ou, na hipótese de a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, os documentos de habilitação anteriormente inseridos no sistema, até a abertura da sessão pública.
- 5.10. Não haverá ordem de classificação na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.
- 5.11. Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para apresentação de propostas, após a fase de envio de lances.
- 5.12. Desde que disponibilizada a funcionalidade no sistema, o licitante poderá parametrizar o seu valor final mínimo ou o seu percentual de desconto máximo quando do cadastramento da proposta e obedecerá às seguintes regras:
- 5.12.1 a aplicação do intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta; e
- 5.12.2 os lances serão de envio automático pelo sistema, respeitado o valor final mínimo, caso estabelecido, e o intervalo de que trata o subitem acima.
- 5.13. O valor final mínimo ou o percentual de desconto final máximo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:
- 5.13.1 valor superior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por menor preço; e
- 5.13.2 percentual de desconto inferior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por maior desconto.
- 5.14. O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do item 5.12 possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.
- 5.15. Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da

perda de negócios diante da inobservância de mensagens emitidas pela Administração ou de sua desconexão.

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

6. DO PREENCHIMENTO DA PROPOSTA

6.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, das seguintes informações:

- 6.1.1 descrição dos serviços de cada item do Grupo/Lote;
- 6.1.2 valor unitário de cada item;
- 6.1.3 Quantidade anual de cada item (quantidade mensal do Termo de Referência x 12);
- 6.1.4 Valor total anual de cada item;
- 6.1.5. Valor total anual do Grupo/Lote.

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

6.2.1 O licitante NÃO poderá oferecer proposta em quantitativo inferior ao máximo previsto para contratação.

6.2.2 A forma de apresentação da proposta no Sistema utilizado para o Pregão, NÃO É a mesma da planilha de custos apresentada no Termo de Referência, devendo o licitante atentar para as orientações acima, uma vez que proposta apresentada de forma divergente incorre na sua desclassificação.

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

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

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

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

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

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

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

6.10. Caso o critério de julgamento seja o de menor preço, os licitantes devem respeitar os preços máximos previstos no Termo de Referência;

6.11. Caso o critério de julgamento seja o de maior desconto, o preço já decorrente da aplicação do desconto ofertado deverá respeitar os preços máximos previstos no Termo de Referência.

6.12. O descumprimento das regras supramencionadas pode ensejar a responsabilização pelo Tribunal de Contas do Estado do Tocantins e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos

responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

6.13. Em se tratando de serviços com fornecimento de mão de obra em regime de dedicação exclusiva, o licitante deverá indicar os sindicatos, acordos coletivos, convenções coletivas ou sentenças normativas que regem as categorias profissionais que executarão o serviço e as respectivas datas bases e vigências, com base na Classificação Brasileira de Ocupações – CBO.

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

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

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

7.3. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro/Agente de Contratação/Comissão e os licitantes.

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

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

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

7.7. O licitante somente poderá oferecer lance de valor inferior ou percentual de desconto superior ao último por ele ofertado e registrado pelo sistema.

7.8. **O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de 0,05% (zero vírgula, zero cinco por cento) do valor total estimado.**

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

7.10. O procedimento seguirá de acordo com o modo de disputa adotado.

7.11. Caso seja adotado para o envio de lances na licitação o modo de disputa “aberto”, os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

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

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

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

7.12. Caso seja adotado para o envio de lances na licitação o modo de disputa “aberto e fechado”, os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

7.12.1 A etapa de lances da sessão pública terá duração inicial de quinze minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de até dez minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.

7.12.2 Encerrado o prazo previsto no subitem anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até 10% (dez por cento) superiores àquela possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

7.12.3 No procedimento de que trata o subitem supra, o licitante poderá optar por manter o seu último lance da etapa aberta, ou por ofertar melhor lance.

7.12.4 Não havendo pelo menos três ofertas nas condições definidas neste item, poderão os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de três, oferecer um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

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

7.13. Caso seja adotado para o envio de lances na licitação o modo de disputa “fechado e aberto”, poderão participar da etapa aberta somente os licitantes que apresentarem a proposta de menor preço/ maior percentual de desconto e os das propostas até 10% (dez por cento) superiores/inferiores àquela, em que os licitantes apresentarão lances públicos e sucessivos, até o encerramento da sessão e eventuais prorrogações.

7.13.1 Não havendo pelo menos 3 (três) propostas nas condições definidas no item 7.13, poderão os licitantes que apresentaram as três melhores propostas, consideradas as empatadas, oferecer novos lances sucessivos.

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

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

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

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

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

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

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

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

7.17. No caso de desconexão com o Pregoeiro/Agente de Contratação/Comissão, no decorrer da etapa competitiva da licitação, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

7.18. Quando a desconexão do sistema eletrônico para o Pregoeiro/Agente de Contratação/Comissão persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo

Pregoeiro/Agente de Contratação/Comissão aos participantes, no sítio eletrônico utilizado para divulgação.

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

7.20. Só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

7.21. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial, caso a contratação não se enquadre nas vedações dos §§1º e 2º do art. 4º da Lei nº 14.133, de 2021. 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 nº 8.538, de 2015, quando aplicável à licitação.

7.21.1 Quando houver propostas beneficiadas com as margens de preferência, apenas poderão se valer do critério de desempate previsto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, as propostas de microempresas e empresas de pequeno porte que também fizerem jus às margens de preferência (art. 5º, §9º, I, do Decreto n.º 8538, de 2015).

7.21.2 O parâmetro para o empate ficto, nesse caso, consistirá no preço ofertado pela fornecedora classificada em primeiro lugar em razão da aplicação da margem de preferência.

7.21.3 Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem naquele intervalo de até 5% (cinco por cento), serão consideradas empatadas com a primeira colocada.

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

7.21.5 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 até 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

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

7.21.7 A obtenção do benefício a que se refere o item anterior fica limitada às microempresas e às empresas de pequeno porte que, no ano-calendário de realização da licitação, 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.

7.22. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60 da Lei nº 14.133, de 2021, nesta ordem:

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

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

7.22.1.3. desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento;

7.22.1.4. desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

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

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

7.22.2.2. empresas brasileiras;

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

7.22.2.4. empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187, de 29 de dezembro de 2009.

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

7.24. Encerrada a etapa de envio de lances da sessão pública, na hipótese da proposta do primeiro colocado permanecer acima do preço máximo ou inferior ao desconto definido para a contratação, o Pregoeiro/Agente de Contratação/Comissão poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

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

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

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

7.25. O Pregoeiro/Agente de Contratação/Comissão solicitará ao licitante mais bem classificado que, **no prazo de 02 (duas) horas**, envie a proposta adequada ao último lance ofertado após a negociação realizada, **acompanhada do comprovante de garantia da proposta**, e documentos com especificações técnicas necessários à confirmação de que atendem aos requisitos básicos de desempenho exigidos neste Edital e seus anexos.

7.25.1. É facultado ao Pregoeiro/Agente de Contratação/Comissão prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

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

7.27. A PROPOSTA REALINHADA DEVERÁ SER APRESENTADA EM CONFORMIDADE COM A PLANILHA CONSTANTE NO TERMO DE REFERÊNCIA, CONTENDO:

a) Descrição de cada item do Grupo/Lote;

b) Quantitativo mensal de cada item;

c) Valor unitário de cada item;

d) Valor total mensal de cada item;

e) Valor total mensal e anual de sua proposta.

7.28. Encerrado o prazo, o Pregoeiro/Agente de Contratação/Comissão iniciará a fase de aceitação e julgamento da proposta.

8. DO JULGAMENTO E DA ACEITABILIDADE DA PROPOSTA VENCEDORA

8.1. Encerrada a etapa de negociação, o Pregoeiro/Agente de Contratação/Comissão verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133, de 2021, legislação correlata e no item 3.7 do Edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

8.1.1 SICAF;

8.1.2 Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (<https://portal.datransparencia.gov.br/pagina-interna/603244-cnep>); e.

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

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

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

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

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

8.4. Na hipótese de inversão das fases de habilitação e julgamento, caso atendidas as condições de participação, será iniciado o procedimento de habilitação.

8.5. Verificadas as condições de participação, o Pregoeiro/Agente de Contratação/Comissão 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.

8.6. Será desclassificada a proposta vencedora que:

8.6.1 conter vícios insanáveis;

8.6.2 não obedecer às especificações técnicas contidas no Termo de Referência;

8.6.3 ofertar marca e modelo de veículo com especificações, e/ou qualidade, e/ou desempenho inferiores aos estipulados no Termo de Referência;

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

8.6.5 não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

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

8.7. E indício de inexequibilidade das propostas, valores inferiores a 50% (cinquenta por cento) do valor total orçado pela Administração para o grupo/lote, bem como para cada item que compõe o grupo/lote.

8.8. A inexequibilidade, na hipótese de que trata o item anterior, só será considerada após diligência do Pregoeiro/Agente de Contratação/Comissão, que comprove:

8.8.1 que o custo do licitante ultrapassa o valor da proposta; e

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

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

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

9. DA HABILITAÇÃO

9.1. Os documentos considerados necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, exigidos para fins de habilitação, com base nos arts. 62 a 70 da Lei nº 14.133, de 2021, são:

9.1.1. Habilitação jurídica

- a) Cédula de Identidade do representante legal da proponente;
- b) Registro comercial, no caso de empresa individual; ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado e com alterações consolidadas, em se tratando de sociedades comerciais, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores; ou inscrição do ato constitutivo, no caso de sociedades civis, acompanhada de prova de diretoria em exercício;
- c) Decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no País, e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir;

9.1.2. Habilitação fiscal, social e trabalhista

- a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas, com situação “ativa”, cujo comprovante tenha sido emitido em até 60 (sessenta) dias, da data da abertura da sessão da licitação;
- b) Prova de regularidade fiscal perante a Fazenda Federal, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB);
- c) Prova de regularidade fiscal perante a fazenda Municipal e Estadual/Distrital, referente ao domicílio ou sede do licitante, relativa à atividade em cujo exercício contrata ou concorre;
- d) Prova de regularidade relativa à Seguridade Social e ao Fundo de Garantia do Tempo de Serviço (FGTS);
- e) Prova de regularidade perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943.

9.1.3. Qualificação Econômico-Financeira

- a) Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor (Lei nº 14.133, de 2021, art. 69, caput, inciso II).

9.1.4. Qualificação Técnica

- a) Declaração de que o fornecedor tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da contratação.
- b) Apresentação de no mínimo um atestado emitido por pessoa jurídica de direito público ou privado, comprovando que a proponente fornece/forneceu serviços compatíveis com os objetos da licitação emitidos em papel timbrado, com assinatura, identificação e telefone do emitente;
 - b.1) Não serão aceitos atestados com objeto genérico, ou seja, deverá constar nos respectivos Atestados nomenclatura compatível com os itens licitados.
 - b.2) Os atestados deverão ser apresentados em papel timbrado ou com carimbo do CNPJ da pessoa jurídica emitente, contendo a identificação do signatário.
 - b.3) Não serão aceitos documentos que representam a participação da licitante em consórcio e/ou cooperativa para fins de qualificação técnica;

b.4) Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente (Acórdão 2939/2021-TCU Plenário);

b.5) Os documentos apresentados estão sujeitos à verificação do Pregoeiro quanto à veracidade dos respectivos conteúdos;

b.6) Caso seja solicitado pelo pregoeiro, o licitante deverá disponibilizar todas as informações necessárias à comprovação da legitimidade dos atestados apresentados, apresentando, dentre outros documentos, Notas Fiscais, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços.

c) Declaração da licitante de que examinou o Termo de Referência em sua integralidade, incluindo as especificações, conhece todos os aspectos peculiares à execução dos serviços, efetuou todas as interpretações, deduções e conclusões para definição do seu custo de execução, de maneira que qualquer eventual falha de sua parte não a isentará das obrigações assumidas, independentemente de sua dificuldade.

9.1.5. Outros documentos

a) Declaração não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7º, XXXIII, da Constituição.

b) Declaração, a ser apresentada no ato do credenciamento na sessão do Pregão, dando ciência de que cumpre plenamente os requisitos de habilitação, na forma do inciso I, do artigo 63, da Lei 14.133/2021;

c) Declaração, de Inexistência de Fato Superveniente Impeditivo da Habilitação;

d) Declaração de Elaboração Independente de Proposta;

e) Declaração de que não possui em seus quadros, empregados que sejam cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de Membros e Servidores ocupantes de cargo de direção, chefia ou assessoramento da Assembleia Legislativa do Tocantins, bem como a prestação de serviço por empregado de empresa fornecedora de mão-de-obra que se enquadre na situação citada acima.

f) Termo de Vistoria Técnica ou Declaração de não realização da Vistoria.

9.1.6. Será verificado se o licitante apresentou no sistema, sob pena de desclassificação, declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei.

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

9.1.8. Caso alguma(s) da(s) declarações acima não constem no Sistema para o licitar assinalar, deverá(ão) ser(em) apresentada(s) juntamente com os demais documentos de habilitação.

9.2. A documentação exigida deverá ter validade no mínimo até a data prevista para abertura do Pregão. Se o prazo de validade das Certidões não estiver expresso, será considerado o prazo de 90 (noventa) dias consecutivos, excluindo-se nesta contagem o dia da emissão/expedição (o primeiro dia na contagem do prazo de validade é o seguinte à sua emissão).

9.3. As certidões obtidas via internet estarão sujeitas à verificação de sua validade e autenticidade pelo(a) Pregoeiro(a). A verificação nos sites oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova.

9.3.1 Caso alguma certidão apresentada esteja com o prazo de validade vencido e haja possibilidade de extrair nova certidão pela internet na própria sessão, a mesma poderá ser imediatamente suprida pelo(a) Pregoeiro (a).

9.4. A habilitação será verificada por meio do SICAF, nos documentos por ele abrangidos.

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

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

9.6. A verificação pelo Pregoeiro/Agente de Contratação/Comissão, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

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

9.8. Os documentos exigidos para habilitação que não estejam contemplados no SICAF deverão ser enviados por meio do sistema, em formato digital, **no prazo de 02 (duas horas)**, prorrogável por igual período, contado da solicitação do Pregoeiro/Agente de Contratação/Comissão.

9.9 Na hipótese de a fase de habilitação anteceder a fase de apresentação de propostas e lances, os licitantes encaminharão, por meio do sistema, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto.

9.10. A verificação no SICAF ou a exigência de encaminhamento dos documentos nele não contidos somente será feita em relação ao licitante vencedor.

9.10.1 Os documentos relativos à regularidade fiscal somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante mais bem classificado.

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

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

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

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

9.12. 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, atribuindo-lhes eficácia para fins de habilitação e classificação.

9.13. Na hipótese de o licitante não atender às exigências para habilitação, o Pregoeiro/Agente de Contratação/Comissão examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital, observado o prazo disposto no subitem 9.8.

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

9.15. A comprovação de regularidade fiscal e trabalhista das microempresas e das empresas de pequeno porte somente será exigida para efeito de contratação, e não como condição para participação na licitação.

9.16. Quando a fase de habilitação anteceder a de julgamento e já tiver sido encerrada, não caberá exclusão de licitante por motivo relacionado à habilitação, salvo em razão de fatos supervenientes ou só conhecidos após o julgamento.

9.17. CERTIFICAÇÕES E CONFORMIDADE DO PROVEDOR DE NUVEM

9.17.1 Encerrada a fase de habilitação e fase recursal, o licitante declarado vencedor deverá encaminhar ao Pregoeiro, para análise e aprovação, ou não, da área técnica do setor demandante da contratação os documentos comprobatórios das Certificações e Conformidade do provedor de nuvem, conforme estipulado no subitem 5.9 do Termo de Referência, anexo I deste Edital.

9.18. PROVA DE CONCEITO

9.18.1 Para a presente contratação, é exigida a apresentação de Prova de Conceito do licitante classificado em primeiro lugar, que deverá apresentá-la conforme disciplinado no item 6 do Termo de Referência, sob pena de desclassificação da proposta.

9.18.2 Por meio de mensagem no sistema, será divulgado o local e horário de realização do procedimento para a avaliação da amostra/Prova de Conceito, cuja presença será facultada a todos os interessados, incluindo os demais licitantes.

9.19. Os resultados das avaliações serão divulgados por meio de mensagem no sistema, e os respectivos documentos elaborados pela equipe técnica responsável pela avaliação, disponibilizados no sítio eletrônico da Assembleia Legislativa do Tocantins: www.al.to.leg.br “licitações”.

9.20. No caso de não haver entrega da amostra/Prova de Conceito ou ocorrer atraso na entrega/realização, sem justificativa aceita pelo Pregoeiro/Agente de Contratação/Comissão, ou havendo entrega de amostra/Prova de Conceito fora das especificações previstas neste Edital, a proposta do licitante será desclassificada.

9.21. Se a Prova de Conceito apresentada pelo primeiro classificado não for aceita pela equipe técnica, o Pregoeiro convocará o segundo classificado, e fará os procedimentos de julgamento da proposta e habilitação, e posteriormente, seguir-se-á com a verificação da Certificação e Conformidade do provedor de nuvem e da Prova de Conceito. E, assim, sucessivamente, até a verificação de uma proposta que atenda às especificações constantes no Termo de Referência.

10. DO TERMO DE CONTRATO

10.1. Após a aprovação da Prova de Conceito, se dará a adjudicação e homologação, e caso se conclua pela contratação, será firmado termo de contrato.

10.2. O adjudicatário terá o prazo de 05 (cinco) dias úteis, contados a partir da data de sua convocação, para assinar o termo de contrato ou instrumento equivalente, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas neste Edital.

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

- a) encaminhá-lo para assinatura, mediante envio de arquivo digital por e-mail, para que seja assinado e devolvido no prazo de 02 (dois) dias úteis, a contar da data de seu recebimento;
- b) outro meio eletrônico, assegurado o prazo de 02 (dois) dias úteis para resposta após recebimento da notificação pela Administração.

10.4. Os prazos dos itens 10.2 e 10.3 poderão ser prorrogados, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

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

10.6. Na assinatura do contrato ou instrumento equivalente será exigido a comprovação das condições de habilitação e contratação consignadas neste Edital, que deverão ser mantidas pelo fornecedor durante a vigência do contrato.

11. DA ATA DE REGISTRO DE PREÇOS

11.1. Homologado o resultado da licitação, o licitante mais bem classificado terá o prazo de 05 (cinco) dias, contados a partir da data de sua convocação, para assinar a Ata de Registro de

Preços, cujo prazo de validade encontra-se nela fixado, sob pena de decadência do direito à contratação, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021.

11.2. O prazo de convocação poderá ser prorrogado uma vez, por igual período, mediante solicitação do licitante mais bem classificado ou do fornecedor convocado, desde que:

11.2.1 a solicitação seja devidamente justificada e apresentada dentro do prazo; e

11.2.2 a justificativa apresentada seja aceita pela Administração.

11.3. A ata de registro de preços poderá ser assinada por meio digital e disponibilizada no sistema de registro de preços.

11.4. Serão formalizadas tantas Atas de Registro de Preços quantas forem necessárias para o registro de todos os itens constantes no Termo de Referência, com a indicação do licitante vencedor, a descrição do(s) item(ns), as respectivas quantidades, preços registrados e demais condições.

11.5. O preço registrado, com a indicação dos fornecedores, será divulgado no PNCP e disponibilizado durante a vigência da ata de registro de preços.

11.6. A existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas, mas não obrigará a Administração a contratar, facultada a realização de licitação específica para a aquisição pretendida, desde que devidamente justificada.

11.7. Na hipótese de o convocado não assinar a ata de registro de preços no prazo e nas condições estabelecidas, fica facultado à Administração convocar os licitantes remanescentes do cadastro de reserva, na ordem de classificação, para fazê-lo em igual prazo e nas condições propostas pelo primeiro classificado.

12. DA FORMAÇÃO DO CADASTRO DE RESERVA

12.1. Após a homologação da licitação, será incluído na ata, na forma de anexo, o registro:

12.1.1 dos licitantes que se manifestarem aceitarem constar de cadastro de reserva, cotando o objeto com preço igual ao do adjudicatário, observada a classificação na licitação; e

12.1.2 dos licitantes que se manifestarem constar de cadastro de reserva, mantendo sua proposta final.

12.2. Será respeitada, nas contratações, a ordem de classificação dos licitantes ou fornecedores registrados na ata.

12.2.1 A apresentação de novas propostas na forma deste item não prejudicará o resultado do certame em relação ao licitante mais bem classificado.

12.2.2 Para fins da ordem de classificação, os licitantes ou fornecedores que aceitarem cotar o objeto com preço igual ao do adjudicatário, antecederão aqueles que mantiverem sua proposta original.

12.3. A habilitação dos licitantes que comporão o cadastro de reserva será efetuada quando houver necessidade de contratação dos licitantes remanescentes, nas seguintes hipóteses:

12.3.1 quando o licitante vencedor não assinar a ata de registro de preços no prazo e nas condições estabelecidos no edital; ou

12.3.2 quando houver o cancelamento do registro do fornecedor ou do registro de preços, nas hipóteses previstas no Decreto nº 552, de 2024.

12.4. Na hipótese de nenhum dos licitantes que aceitaram cotar o objeto com preço igual ao do adjudicatário concordar com a contratação nos termos em igual prazo e nas condições propostas pelo primeiro classificado, a Administração, observados o valor estimado e a sua eventual atualização na forma prevista no edital, poderá:

12.4.1 convocar os licitantes que mantiveram sua proposta final para negociação, na ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário; ou

12.4.2 adjudicar e firmar o contrato nas condições ofertadas pelos licitantes remanescentes, observada a ordem de classificação, quando frustrada a negociação de melhor condição.

13. DOS RECURSOS

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

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

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

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

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

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

13.3.4 na hipótese de adoção da inversão de fases prevista no § 1º do art. 17 da Lei nº 14.133, de 2021, o prazo para apresentação das razões recursais será iniciado na data de intimação da ata de julgamento.

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

13.5. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá reconsiderar sua decisão no prazo de 3 (três) dias úteis, ou, nesse mesmo prazo, encaminhar recurso para a autoridade superior, a qual deverá proferir sua decisão no prazo de 10 (dez) dias úteis, contado do recebimento dos autos.

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

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

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

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

13.10. Os autos do processo permanecerão com vista franqueada aos interessados na Diretoria de Licitação, Anexo I da Assembleia Legislativa do Tocantins, Rua de Pedestres NE 03, Quadra 104 Norte, nº 35, P. D. Norte, Palmas – TO.

14. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

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

14.1.1 deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo Pregoeiro/Agente de Contratação/Comissão durante o certame;

14.1.2 salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta em especial quando:

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

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

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

14.1.2.4. deixar de apresentar amostra;

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

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

- 14.1.4 recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;
- 14.1.5 apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação;
- 14.1.6 fraudar a licitação;
- 14.1.7 comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:
- 14.1.7.1. agir em conluio ou em desconformidade com a lei;
- 14.1.7.2. induzir deliberadamente a erro no julgamento;
- 14.1.7.3. apresentar amostra falsificada ou deteriorada.
- 14.1.8 praticar atos ilícitos com vistas a frustrar os objetivos da licitação;
- 14.1.9 praticar ato lesivo previsto no art. 5º da Lei n.º 12.846, de 2013.
- 14.2. Com fulcro na Lei nº 14.133, de 2021, a Administração poderá, após regular processo administrativo, garantida a prévia defesa, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:
- 14.2.1 advertência;
- 14.2.2 multa;
- 14.2.3 impedimento de licitar e contratar e
- 14.2.4 declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.
- 14.3. Na aplicação das sanções serão considerados:
- 14.3.1 a natureza e a gravidade da infração cometida;
- 14.3.2 as peculiaridades do caso concreto;
- 14.3.3 as circunstâncias agravantes ou atenuantes;
- 14.3.4 os danos que dela provierem para a Administração Pública;
- 14.3.5 a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.
- 14.4. A multa será recolhida no prazo máximo de **10 (dez) dias úteis**, a contar da comunicação oficial.
- 14.4.1 Para as infrações previstas nos itens 14.1.1, 14.1.2 e 14.1.3, a multa será de 0,5% a 15% do valor do contrato licitado.
- 14.4.2 Para as infrações previstas nos itens 14.1.5, 14.1.6, 14.1.7, 14.1.8 e 14.1.9, a multa será de 15% a 30% do valor do contrato licitado.
- 14.5. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.
- 14.6. Na aplicação da sanção de multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.
- 14.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 14.1.1, 14.1.2 e 14.1.3, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo a qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.
- 14.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 14.1.5, 14.1.6, 14.1.7, 14.1.8 e 14.1.9, bem como pelas infrações administrativas previstas nos itens 14.1.1, 14.1.2 e 14.1.3 que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de

licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei n.º 14.133, de 2021.

14.9. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no item 14.1.3, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação.

14.10. A apuração de responsabilidade relacionadas às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta por 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o adjudicatário para, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

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

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

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

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

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

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

15. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

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

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

15.3. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica, através do e-mail: cpl@al.to.leg.br.

15.3.1. Recebidos os eventuais pedidos de impugnações e/ou esclarecimentos, o Pregoeiro os disponibilizará em campo próprio no Sistema utilizado na licitação e no sítio oficial da Aleto: www.al.to.leg.br “licitações”, com as respectivas respostas, para conhecimento dos licitantes interessados no certame.

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

15.5. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo Pregoeiro/Agente de Contratação/Comissão, nos autos do processo de licitação.

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

16. DA GARANTIA DA PROPOSTA

16.1 Será exigido das licitantes, conforme previsto no artigo 58, da Lei 14.133/2021, garantia da proposta equivalente a 1% (um por cento) do valor estimado para a contratação a que concorre, podendo a licitante optar por uma das seguintes modalidades (artigo 96, parágrafo 1º da Lei 14.133/2021):

I - caução em dinheiro ou em títulos da dívida pública emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados por seus valores econômicos, conforme definido pelo Ministério da Economia;

II - seguro-garantia;

III - fiança bancária emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil.

16.2 O documento oficial comprobatório da garantia da proposta deverá ser anexado juntamente com a proposta ajustada ao preço final, cuja ausência ensejará na desclassificação da proposta do licitante.

16.2.1 O prazo de validade da garantia por meio de Seguro-Garantia ou Fiança bancária, será de no mínimo 90 (noventa) dias após o prazo de vigência da proposta.

16.2.2. A garantia em dinheiro das licitantes não vencedoras ser-lhes-ão restituídas no prazo de até 10 (dez) dias úteis, contado a partir da homologação da licitação.

16.2.3 A garantia das licitantes inabilitadas ser-lhes-ão restituídas no prazo de 05 (cinco) dias úteis, contado a partir do encerramento da fase de habilitação; em caso de interposição de recursos, o prazo de devolução será contado a partir do julgamento definitivo dos recursos.

16.2.4. A garantia da empresa vencedora, será devolvida no prazo de até 10 (dez) dias úteis após a assinatura do Contrato.

17. DA VISTORIA/VISITA TÉCNICA

17.1 - É facultado à proponente realizar vistoria técnica na Sede da Assembleia Legislativa, localizado na cidade de Palmas - TO, em data agendada para levantamento de informações sobre o local onde estão atualmente instalados os equipamentos de TIC e onde deverá ser instalado o circuito do link LAN-TO-LAN, com intuito de avaliar os serviços e entregas que serão exigidas posteriormente se declarada como vencedora da disputa;

17.2. As empresas deverão solicitar o agendamento da vistoria em até 4 (quatro) dias úteis da data da disputa, pelo e-mail cosuti@al.to.leg.br, cujo campo “assunto” da mensagem deverá conter o texto “Vistoria – Edital Serviços de Cloud Computing”. As empresas serão comunicadas por e-mail, dos momentos e local onde devem se apresentar, para a vistoria, e quem as conduzirá. A vistoria será realizada em até 3 (três) dias úteis da data do certame;

17.3. Ao final da vistoria, a Aleto emitirá Termo em favor da proponente, circunstanciando o atendimento desta exigência. Os custos da vistoria são de responsabilidade da proponente, incluindo seus deslocamentos em veículo próprio ao local vistoriado;

17.4. Caso a proponente opte por não realizar vistoria, firmará declaração na qual dispensa a necessidade de vistoria, assumindo todo e qualquer risco por sua decisão e se comprometendo a prestar fielmente o serviço nos termos de sua proposta e do Edital e seus Anexos.

17.5. O Termo de Vistoria Técnica ou a Declaração de Dispensa de Vistoria deverá ser apresentado juntamente com a documentação relativa à habilitação do certame. Não será

permitida a participação de empresas que não atenderam esta exigência, estando automaticamente desclassificadas do certame.

18. DA DOTAÇÃO ORÇAMENTÁRIA

18.1 - As aquisições decorrentes da presente contratação serão pagas com recursos previstos no orçamento desta Assembleia Legislativa, conforme Dotação orçamentária indicada autos.

19. DAS DISPOSIÇÕES GERAIS

19.1 - Será divulgada ata da sessão pública no sistema eletrônico.

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

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

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

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

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

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

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

19.9 - É facultado ao pregoeiro ou a autoridade competente, em qualquer fase do julgamento promover diligência destinada a esclarecer ou complementar a instrução do processo e a aferição do produto ofertado, bem como solicitar a órgãos competentes a elaboração de pareceres técnicos destinados a fundamentar as decisões.

19.10 – Qualquer solicitação de prorrogação de prazo para execução do objeto, decorrentes desta licitação, somente será analisada se apresentada antes do decurso do prazo para tal e devidamente fundamentada.

19.11 – A administração reserva a si o direito de revogar a presente licitação por razões de interesse público ou anulá-la, no todo ou em parte por vício ou ilegalidade, bem como prorrogar o prazo para recebimento das propostas e/ou sessão de lances, desqualificar qualquer licitante ou desclassificar qualquer proposta, caso tome conhecimento de fato que afete a capacidade financeira, técnica ou comercial da licitante, sem que isto gere direito à indenização ou ressarcimento de qualquer natureza.

19.12 - O pregoeiro, no interesse da Administração, poderá relevar omissões puramente formais observadas na documentação e proposta, desde que não contrariem a legislação vigente e não comprometam a lisura da licitação, sendo possível a promoção de diligência destinada a esclarecer ou a complementar a instrução do processo.

19.13 - O licitante deverá examinar detidamente as disposições contidas neste Edital e seus anexos, pois o simples registro de proposta financeira junto ao sistema eletrônico de licitação utilizado, submete-a à aceitação incondicional de seus termos, independente de transcrição, bem

como representa o conhecimento do objeto em licitação e a observância dos preceitos legais e regulamentares que a regem, não sendo aceita alegação de desconhecimento de qualquer pormenor.

19.14. É vedado ao fornecedor retirar sua proposta ou parte dela após aberta a sessão do pregão.

19.15. É vedado a qualquer licitante tentar impedir o curso normal do processo licitatório mediante a utilização de recursos ou de meios meramente protelatórios, sujeitando-se o autor às sanções legais e administrativas.

19.16. Informações sobre o andamento da licitação poderão ser obtidas junto à Diretoria de Licitação, nos dias úteis, em horário de expediente pelo e-mail: cpl@al.to.leg.br. Ainda, poderão ser acompanhadas as fases através do sistema utilizado no Pregão.

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

19.18 - O Edital e seus anexos estarão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP), no endereço eletrônico www.al.to.leg.br “licitacao” e no sistema utilizado neste pregão. Também poderão ser lidos e/ou obtidos no endereço: Anexo I da Assembleia Legislativa, na Quadra 104 Norte, Rua NE 03, Lote 35, 2º andar, Palmas, Estado do Tocantins, nos dias úteis, no horário de expediente ao público, mesmo endereço e período no qual os autos do processo administrativo permanecerão com vista franqueada aos interessados.

19.19 - Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

19.19.1 - ANEXO I - Termo de Referência

19.19.2 - ANEXO II – Minuta da Ata de Registro de Preços

19.19.3 – ANEXO III - Minuta do Termo de Contrato

Palmas, 03 de junho de 2025

Jorge Mário Soares de Sousa
Diretor de Licitação

ANEXO I
TERMO DE REFERÊNCIA
PROCESSO Nº 217/2025
INTRODUÇÃO

Este documento será elaborado fundamentado nos preceitos da Lei Federal 14.133 de 1º de abril de 2021, concomitante com o Decreto Administrativo 552/24 de 05 de junho de 2024

1. OBJETO DA CONTRATAÇÃO (Anexo III, Art. 6º, Inciso I do Decreto 552/24)

1.1. Definição do Objeto: A Assembleia Legislativa do Estado do Tocantins busca estabelecer uma ata de registro de preços para a futura contratação, de empresa especializada na prestação de serviços de CLOUD COMPUTING de infraestrutura TIC, baseado na plataforma IaaS (Infraestrutura como serviço).

1.2. Do prazo do Contrato: O contrato terá prazo inicial de 12 meses, podendo ser prorrogado por períodos sucessivos até o limite que está preconizado na Seção VII, Art. 79, Inciso IV, do Decreto Administrativo 552/24.

A ARP gerada à partir do processo licitatório, terá validade de 12 meses podendo ser prorrogada por igual período, enquanto tiver validade de acordo com o Art.40 do Decreto 552/24.

1.3. Do prazo para inicialização dos serviços: O prazo para execução dos serviços será detalhado no tópico “MODELO DE EXECUÇÃO DO OBJETO”.

1.4. Da Natureza do serviço: Trata-se de serviços de natureza continuada sem dedicação exclusiva de mão-de-obra.

Nos termos do inciso XIII, do art. 6º, da lei 14.133, de 2021, os serviços desta contratação são caracterizados como comuns, em vista da possibilidade de definição objetiva dos padrões de desempenho e de qualidade, conforme prática usual no mercado, conforme justificativa constante do Estudo Técnico Preliminar.

Esta contratação de Solução de Computação em Nuvens Públicas é destinada à prestação de serviços técnicos especializados de natureza contínua na área de infraestrutura de Tecnologia da Informação (TI), ao se considerar a complexidade, essencialidade, o necessário período de estabilização dos serviços que fazem parte do objeto da solução pretendida.

A aquisição dos serviços que serão descritos nesse documento, não irão gerar vínculo empregatício entre os empregados da Contratada e a Administração, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

1.5. Do prazo de Garantia Deverá contar com serviço de suporte 24 x 7 (vinte e quatro horas por dia, sete dias por semana), prestado diretamente pelo provedor do serviço, e garantia para defeitos de fabricação durante todo o período do contrato, de forma que a prestação dos serviços não seja interrompida, contemplando toda a solução ofertada.

1.6. Do Local da prestação dos Serviços: Os serviços serão executados na Sede da Assembleia Legislativa do Estado do Tocantins, localizada em: Palácio Deputado João D'Abreu - Praça dos Girassóis, s/n - Plano Diretor Norte, Palmas - TO, 77001-902

2. ESPECIFICAÇÃO DO PRODUTO E QUANTITATIVOS (Incisos XIV e XV do Decreto 552/2024, Anexo III)

LOTE ÚNICO			
ITEM	DESCRIÇÃO DOS SERVIÇOS	UNIDADE	QTDE
1	SERVIÇOS DE VCPU	Serviço/mês	200
2	SERVIÇOS DE MEMORIA RAM (GB)	Serviço/mês	400
3	SERVIÇOS DE ARMAZENAMENTO EM BLOCO NVME (GB)	Serviço/mês	12.000
4	SERVIÇOS DE ARMAZENAMENTO EM BLOCO HDD (GB)	Serviço/mês	70.000
5	SERVIÇOS DE LINK LAN-TO-LAN (MB)	Serviço/mês	1.000

6	SERVIÇOS DE LINK DE INTERNET (MB)	Serviço/mês	1.000
7	SERVIÇOS DE LICENÇAS WINDOWS SERVER	Serviço/mês	80
08	SERVIÇOS GERENCIADOS DE FIREWALL	Serviço/mês	2
09	SERVIÇOS GERENCIADOS DE ANTIVÍRUS	Serviço/mês	50
10	SERVIÇOS GERENCIADOS DE BACKUP	Serviço/mês	50
11	SERVIÇOS DE NOC (PCT 10 ATIVOS)	Serviço/mês	50
12	SERVIÇOS TÉCNICOS ESPECIALIZADOS (HORAS)	Serviço/horas	80

2.1. ESPECIFICAÇÕES DO AMBIENTE DE DATA CENTER

2.1.1. Características Gerais (Físicas do Contratado)

2.1.1.1. O serviço deverá prover infraestrutura de sustentação operacional e atender características técnicas construtivas para a prestação do Serviço de Cloud Computig compostas pelas especificações e normas técnicas indicadas nos itens adiantes;

2.1.1.2. O espaço físico deverá possuir piso elevado com resistência mínima para acomodar a carga do rack mesmo que estes estejam completamente ocupados por equipamentos;

2.1.1.3. Deverá possuir Racks com porta frontal com controle de acesso e demarcação com patch panels, leitos e calhas sob piso elevado ou aéreo para passagem de cabeamento metálico ou óptico. O perímetro deverá delimitar espaço suficiente para conforto de acesso aos equipamentos nos racks pelos especialistas TIC da CONTRATANTE;

2.1.1.4. A CONTRATADA deverá fornecer segurança física com equipe de vigilância patrimonial 24 horas por dia, 7 dias na semana, 365 dias por ano, e sistema composto por câmeras de circuito interno de televisão, monitoradas e gerenciadas, cujas imagens possam ser posteriormente consultadas, por período mínimo de 30 dias, e viabilizem o rastreamento de pessoas dentro do ambiente hospedeiro;

2.1.1.5. A CONTRATADA deverá ter pessoas dedicadas, treinadas e responsáveis pela segurança de acesso às suas instalações prediais, através de mecanismos efetivos de controle de entrada e saída de pessoas e E

2.1.1.6. O acesso de terceiros aos equipamentos da Contratante se dará sempre mediante autorização expressa da fiscalização/gestão da Contratante;

2.1.1.7. Toda a infraestrutura de DATA CENTER que irá hospedar os dados da CONTRATANTE deve estar sediada no Brasil e possuir capacidade de alta disponibilidade;

2.1.2. Instalações elétricas:

2.1.2.1. A rede elétrica estabilizada 3F+N+T com disponibilidade de circuitos para, bifásica (220V) considerada tolerância de 5%, frequência de 60 Hz com tolerância de 1%, distorção harmônica total menor que 5%, com dois circuitos elétricos independentes e dedicados (Via A e Via B), para alimentação das fontes redundantes dos equipamentos e até 32 tomadas por rack;

2.1.2.2. O padrão de tomadas elétricas adotado será acordado entre a CONTRATADA e a CONTRATANTE em momento anterior à instalação;

2.1.2.3. Deverá atender a tensão de flutuação entre terra e neutro menor que 1,0 volts. Aterramento disponível em todos os racks com valor de impedância menor que 5 ohms;

2.1.2.4. Deverá fornecer a potência elétrica total para alimentação dos equipamentos TIC existentes na infraestrutura atual da CONTRATANTE e que possam vir a ser adquiridos.

2.1.2.5. O cabeamento elétrico deverá ser distribuído através de eletrocalhas devendo todas estarem devidamente aterradas;

2.1.2.6. A estrutura do próprio piso elevado deverá estar adequadamente aterrada para eliminar o acúmulo de carga estática, evitando a ocorrência de descarga eletrostática ESD (Electrostatic Discharge) e o subsequente dano aos equipamentos;

2.1.2.7. Toda a infraestrutura metálica deverá estar interligada e aterrada;

2.1.2.8. Deverá possuir 2 (dois) pontos de entrada de energia elétrica a partir de subestações de eletricidade distintas. Na hipótese de inviabilidade legal, ou seja, leis que impeçam a chegada de 2 subestações de energia distintas em determinada localidade, ou inviabilidade técnica, a CONTRATADA deverá possuir dois alimentadores principais independentes provenientes da mesma subestação;

2.1.2.9. Deverá fornecer Grupo de UPS (Uninterruptible Power Supply) com bancos redundantes e autonomia mínima de 10 (dez) minutos a plena carga;

2.1.2.10. O Grupo UPS deverá ser alimentado por grupo-gerador redundante e independente, que energize toda a área do Data Center (e não apenas os circuitos de alimentação dos nobreaks), com acionamento automático na eventualidade de interrupção no fornecimento de energia comercial e autonomia mínima de 12 (doze) horas, sem reabastecimento;

2.1.2.11. Grupos de Geradores e UPS devem ser redundantes e independentes (n+1 e UPS N+1), com acionamento automático na eventualidade de interrupção no fornecimento de energia, com a capacidade de suportar todo o ambiente por 5 (cinco) dias ininterruptos em caso de falha total no fornecimento de energia elétrica.

2.1.3. Sistema de Climatização:

2.1.3.1. Deverá possuir ar condicionado de precisão com arquitetura redundante (n+1), além das principais, com controles de temperatura, umidade relativa do ar e filtros de poeira, prezando sempre pela manutenção da condição ideal para o bom funcionamento dos equipamentos;

2.1.3.2. Deverá prover temperatura média: 22 graus Celsius (variação máxima de 10%) e umidade relativa do ar em 45% (variação máxima de 10%).

2.1.4. Características do Cabeamento Estruturado LAN/SAN:

2.1.4.1. Toda a infraestrutura de cabeamento estruturado LAN/SAN interior da área Cloud Computing para conectividade dos equipamentos TIC da Contratante será de responsabilidade da CONTRATADA, compreendendo o fornecimento e manutenção ao cabeamento do tipo CAT6 e CAT6A - TIA/EIA-568-C.1 e TIA/EIA-568-C.2, patch panels e patch cords, bem com serviço de cabeamento do tipo fibra óptica OM2, OM3 e OM4, multimode ou singlemode, contemplando distribuidores ópticos e patch cords;

2.1.4.2. Todo o cabeamento estruturado deve ser do tipo LSZH (Low Smoke Zero Halogen), CMP, COP (Plenum) ou outros que apresentem melhor comportamento em relação à propagação vertical e horizontal de chama, densidade de fumaça e gases gerados em sua combustão;

2.1.4.3. Deverá trabalhar com certificação de cabeamento segundo as normas da ANSI/EIA/TIA e ISO/IEC. A certificação deverá ser realizada por um instrumento de análise denominado cable scanner que forneça relatório das características verificadas (exemplos: atenuação, NEXT, PS NEXT, ELFEXT, PSELFEXT e perda de retorno);

2.1.4.4. O Data Center da CONTRATADA deverá possuir sala de entrada secundária para os serviços de telecomunicações, com canaletas redundantes e painéis, tomadas, cabeamento, patch cords e jumpers etiquetados/identificados;

2.1.4.5. O Data Center da CONTRATADA deverá prover facilidades, acessos e conexões, tais como golden jumper e/ou última milha, para que as operadoras de telecomunicação ou prestadores de serviços dessa natureza entreguem circuitos de comunicação de dados que sejam para atender interesses da Contratante, não podendo haver cobrança ou custos adicionais a CONTRATANTE;

2.1.4.6. A CONTRATADA deverá disponibilizar a ativação de GOLDEN JUMPER em até 10 dias úteis;

2.1.4.7. A instalação e sustentação dos equipamentos das operadoras de serviços de comunicação de dados é obrigatória para viabilizar os enlaces de comunicação da CONTRATANTE. O pleno funcionamento desses ativos é regulado por acordo entre as operadoras e a CONTRATADA. Nesses acordos as operadoras instalam estruturas de concentração que podem ser utilizados para outros clientes dos serviços de seu Data Center, não sendo de uso exclusivo da CONTRATANTE. Estes

equipamentos deverão estar instalados em espaço específico (sala segregada) para “TELECOM” e não fazem parte do conjunto de equipamentos alvo do serviço reservado à CONTRATANTE, não sendo sua instalação e sustentação alvo de qualquer cobrança.

2.1.5. Sistema de Controle de Acesso e Monitoramento:

2.1.5.1. A porta de entrada do Colocation deverá possuir fechadura eletrônica;

2.1.5.2. O Colocation deverá possuir Sistema de CFTV digital com recurso de infravermelho para casos de ausência de iluminação para monitoramento remoto da área interna do Colocation;

2.1.5.3. As câmeras deverão ser posicionadas para a visualização do acesso frontal e traseiro dos racks;

2.1.5.4. Deverá haver sistema de gravação digital das imagens com disponibilidade destas por período mínimo de 30 (trinta) dias;

2.1.5.5. É de responsabilidade da CONTRATADA todo o controle de acesso físico de profissionais e materiais às suas instalações e a área Cloud Computing, o qual a Contratante também realizará o monitoramento através de câmeras e demais itens de segurança de perímetro;

2.1.5.6. Os controles de acesso físico ao ambiente devem permitir individualizar o acesso (quem, quando, por que) mantendo o registro para consulta durante toda a vigência do contrato;

2.1.5.7. A CONTRATADA deverá apresentar, sempre que solicitado, informações sobre os procedimentos adotados para armazenamento e gerência dos dados de autenticação, acesso e monitoramento (biometria, chaves de acesso, imagens do CFTV) que impactem na segurança do Colocation contratado;

2.1.5.8. A CONTRATADA deverá possuir sistema de controle de acesso às chaves dos racks (ex.: claviculário eletrônico), devendo a CONTRATADA emitir mensalmente relatório com informações de acesso às chaves dos racks e encaminhar para CONTRATANTE;

2.1.5.9. Deverá possuir sistema de monitoramento ambiental com sensores para monitoramento da temperatura ambiente, umidade do ar e abertura/fechamento da porta do ambiente.

2.1.6. Características dos Serviços de Infraestrutura em Cloud Computing

2.1.6.1. O Data Center deve possuir infraestrutura necessária para disponibilizar o serviço de Cloud Computing de máquinas virtuais com os sistemas operacionais, banco de dados, redes, armazenamento, backups dos dados e das máquinas virtuais, gerenciamento, comunicação, segurança, monitoramento e demais insumos necessários para o processamento dos sistemas da CONTRATANTE;

2.1.6.2. Todos os equipamentos, softwares, infraestrutura e sustentação, necessários à implementação da solução proposta, são de inteira responsabilidade da CONTRATADA, que deverá realizar de forma continuada tarefas e rotinas que garantam o pleno funcionamento de toda a infraestrutura, de forma integral e ininterrupta, ou seja, "24x7x365" (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano) no ambiente de Cloud Computing, mantendo em pleno funcionamento todo objeto da contratação;

2.1.6.3. Toda estrutura do ambiente de Cloud Computing deve ter capacidade de responder ao SLA de pelo menos 99,9%;

2.1.6.4. A CONTRATADA deverá gerenciar, monitorar, sustentar e operar de forma proativa todos os recursos disponibilizados para o CONTRATANTE, de forma a garantir o correto funcionamento de todas as funcionalidades especificadas neste Termo de Referência, em regime 24 x 7 (24 horas por dia, 7 dias por semana);

2.1.6.5. A solução deverá ser escalável, de forma a permitir aumentar ou diminuir os recursos na infraestrutura de Cloud Computing da CONTRATADA para absorver as demandas existentes e novas demandas;

2.1.6.6. Os serviços de Cloud Computing a serem prestados deverão ser baseados em infraestrutura de Data Center, que deverá manter compatibilidade com padrões internacionais, e deverão manter compatibilidade durante toda vigência do contrato com os requisitos abaixo descritos;

2.1.6.7. O ambiente de Cloud Computing deve atender ao modelo IaaS (Infrastructure as a Service - Infraestrutura como um Serviço), e atender os seguintes requisitos:

2.1.6.8. Máquinas virtuais devem possibilitar a utilização de sistemas operacionais Windows e Linux;

2.1.6.9. A disponibilidade das máquinas virtuais deve responder ao SLA de pelo menos 99,99%, calculados mensalmente;

2.1.6.10. Máquinas virtuais devem ser compatíveis com formato padrão de virtualização VHD (Virtual Hard Disk), sem a necessidade de uso de ferramentas de conversão. Permitindo flexibilidade de utilizar o mesmo arquivo de máquina virtual em ambiente de nuvem e ambiente on-premise (local);

2.1.6.11. Deve permitir a criação interfaces de rede virtual em velocidades de 1Gbps ou 10Gbps;

2.1.6.12. A Plataforma deve prover mecanismos de automação de gestão de máquinas virtuais com serviços como criação, inicialização, paralização e remoção de máquinas automaticamente através de execução de script ou ferramenta de orquestração;

2.1.6.13. A Plataforma deve prover mecanismos de alertas baseados no gerenciamento de métricas. Caso uma métrica (uso de disco, processamento, rede, etc) exceda um certo valor, um alerta deve ser gerado e um e-mail, telegram e whatsapp.

2.1.6.14. Implementar características de escalabilidade horizontal (novos servidores) e vertical (aumento de recursos do mesmo servidor), flexibilidade de configuração de memória, processador e disco;

2.1.6.15. Implementar a movimentação automática de servidores virtuais para redistribuição de carga e recuperação de falhas do ambiente;

2.1.6.16. Deverá disponibilizar painel, para gerenciamento de todos servidores, com as funcionalidades de criar maquina, iniciar, desligar, redimensionar configuração, snapshot, criação de usuário para acesso ao painel com controle de permissão de cada usuário;

2.1.6.17. O Ambiente de cloud deverá ser entregue com 2 interfaces, sendo uma para cloud pública e outra para cloud privada, podendo ser adicionado vlans conforme solicitação;

2.1.6.18. O Ambiente de cloud publica, deverá possuir proteção DDOS, para proteção dos serviços publicados;

2.1.6.19. A CONTRATADA deve possuir um segundo DATA CENTER, podendo este ser próprio ou terceirizado, com certificação TIER3, para ser utilizado em casos de necessidade de Disaster Recovery do DATA CENTER onde os serviços de Cloud Computing estão sendo executados. Deverá ser apresentado junto com a proposta comercial um documento que indique a certificação do segundo DATA CENTER, quando próprio ou terceirizado. Em caso de terceirização, a contratada deverá apresentar também o contrato firmado com o provedor de serviços de Data Center, sendo aceito também declaração deste sobre a prestação de serviços à CONTRATADA.

2.2. ITEM 1 – SERVIÇOS VCPU

2.2.1. Características Gerais

2.2.1.1. Deve ser fornecido recursos de vCPUs possibilitando alocação das mesmas para a criação de instâncias virtuais;

2.2.1.2. As vCPUs devem estar baseadas em processadores com arquitetura x86 de pelo menos 2.5 GHz para proporcionar uma boa velocidade de processamento;

2.2.1.3. A razão vCPU:pCPU máxima admitida deve ser de 4:1, ou seja, para cada CPU física (pCPU) no servidor host, no máximo, serão alocadas quatro CPUs virtuais (vCPU) para as máquinas virtuais;

2.2.1.4. Cada unidade deste item representa 1 (uma) vCPU, sendo permitido à CONTRATADA ter a flexibilidade de contratar a quantidade de itens de vCPUs que deverão ser entregues pela CONTRATANTE para serem alocadas nas instâncias de servidores que serão utilizadas.

2.3. ITEM 02 – SERVIÇOS DE MEMÓRIA RAM

2.3.1. Características Gerais

2.3.1.1. Deve ser fornecido recursos de Memória RAM possibilitando alocação das mesmas para a criação de instâncias virtuais;

2.3.1.2. Cada unidade deste item representa 1 GB (Gigabyte), sendo permitido à CONTRATADA ter a flexibilidade de contratar a quantidade de itens de GB que deverão ser entregues pela CONTRATANTE para serem alocadas nas instâncias de servidores que serão utilizadas;

2.3.1.3. As memórias disponibilizadas deverão ser do tipo DDR4-3200 MHz ou superior e possuírem tecnologia ECC (Error-Correcting Code), para maior confiabilidade e integridade dos dados.

2.4. ITEM 03 – SERVIÇOS DE ARMAZENAMENTOS EM BLOCO NVME

2.4.1. Características Gerais

2.4.1.1. Deve ser fornecido recursos de volume block-level de armazenamento baseado em discos do tipo flash NVME possibilitando alocação dos mesmos para a criação de instâncias de servidores virtuais;

2.4.1.2. Cada unidade deste item representa 1 GB (gigabyte), sendo permitido à CONTRATADA ter a flexibilidade de contratar a quantidade de itens de GB que deverão ser entregues pela CONTRATANTE para serem alocadas nas instâncias de servidores que serão utilizadas;

2.4.1.3. Deverá possibilitar que o volume criado seja anexado às máquinas virtuais e reconhecido pelo SO como um dispositivo físico e local;

2.4.1.4. Deverá permitir a definição de nomes ou identificadores de volume de armazenamento;

2.4.1.5. Deverá possuir função de criptografia do volume com mudança de chave gerenciada pela CONTRATADA ou pela CONTRATANTE.

2.5. ITEM 4 – SERVIÇOS DE ARMAZENAMENTO EM BLOCO HDD

2.5.1. Características Gerais

2.5.1.1. Deve ser fornecido recursos de volume block-level de armazenamento baseado em discos do tipo flash NVME possibilitando alocação dos mesmos para a criação de instâncias de servidores virtuais;

2.5.1.2. Cada unidade deste item representa 1 GB (gigabyte), sendo permitido à CONTRATADA ter a flexibilidade de contratar a quantidade de itens de GB que deverão ser entregues pela CONTRATANTE para serem alocadas nas instâncias de servidores que serão utilizadas;

2.5.1.3. Deverá possibilitar que o volume criado seja anexado às máquinas virtuais e reconhecido pelo SO como um dispositivo físico e local;

2.5.1.4. Deverá permitir a definição de nomes ou identificadores de volume de armazenamento;

2.5.1.5. Deverá possuir função de criptografia do volume com mudança de chave gerenciada pela CONTRATADA ou pela CONTRATANTE.

2.6. ITEM 5 – SERVIÇOS DE LAN-TO-LAN

2.6.1. Características Gerais

2.6.1.1. Deve ser fornecido 1 (um) canal principal de comunicação Ponto-a-Ponto para a interligação da LAN do DATA CENTER à Sede da CONTRATANTE, localizada na praça dos Girassóis S/Nº, CEP 77001-902, na cidade de Palmas;

2.6.1.2. O serviço deverá ser prestado mediante implantação do link de comunicação de dados ponto-a-ponto, incluindo o fornecimento de equipamentos e a prestação de suporte técnico;

2.6.1.3. Cada unidade deste item representa 1 (um) Mbps megabits por segundo de capacidade de conexão, sendo permitido à CONTRATADA ter a flexibilidade de contratar a quantidade de itens de 1Mbps, não inferior a 300 (trezentas) unidades, que irá definir a velocidade do link que deverá ser entregue pela CONTRATANTE;

2.6.1.4. Deve garantir uma latência máxima de 5 ms entre os pontos de origem e destino para manter a qualidade das comunicações;

2.6.1.5. A disponibilidade mínima do link deve ser de 99.4% para garantir a conectividade confiável entre as redes;

2.6.1.6. A taxa de perda de pacotes deve ser igual ou inferior a 2%;

2.6.1.7. Todos os equipamentos/cabos devem ser homologados pela ANATEL.

2.6.1.8. Somente em caso de inoperância do canal principal de comunicação de dados ponto-a-ponto entre a LAN do DATA CENTER e a Sede da CONTRATANTE, a comunicação deverá ser automaticamente direcionada para uma rede privada virtual (Virtual Private Network – VPN), com protocolo IPSec e banda mínima de 50 Mbps (Megabits por segundo), provido via infraestrutura de rede INTERNET, para replicação de dados entre as mesmas, garantindo a disponibilidade, segurança, a autenticação das partes interligadas e a criptografia dos dados que trafegam entre elas, sendo o tempo de operação da solução através de conexão VPN computados como período de indisponibilidade da conexão principal de dados ponto-a-ponto entre o provedor e a sede da CONTRATANTE;

2.6.1.9. A taxa de transmissão do canal deverá estar sempre disponível na totalidade do fluxo contratado no período;

2.6.1.10. A CONTRATADA deverá fornecer canal com transmissão full duplex e taxa simétrica, isto é, tenha a mesma capacidade de transmissão para o tráfego de entrada e de saída, simultaneamente;

2.6.1.11. Os canais de comunicação devem ser providos por meio de acessos terrestres, cabos metálicos, cabos ópticos ou enlaces de rádio digital, desde que possuam frequência regulamentada pela ANATEL;

2.6.1.12. Não será permitido o fornecimento de enlaces via satélite, nem a utilização de agregação de várias portas no roteador, pois a conexão deve ser fornecida utilizando uma única interface;

2.6.1.13. O canal principal de comunicação deve possuir conexão permanente, ponto-a-ponto e exclusiva, desde as dependências da sede da CONTRATANTE até a LAN do DATA CENTER, obedecendo às recomendações elaboradas pela EIA/TIA (Electronic Industries Alliance / Telecommunications Industry Association), pela ABNT (Associação Brasileira de Normas Técnicas) e demais normas, quando pertinentes;

2.6.1.14. O canal e os roteadores deverão ser instalados na sala de equipamentos da CONTRATANTE;

2.6.1.15. A CONTRATADA deverá fornecer para a CONTRATANTE um meio on-line de consulta, com segurança de acesso, com informações de desempenho, latência, perda de pacote e ocupação do canal principal de comunicação ponto-a-ponto fornecido, gráficos de tendências e horários de maior e menor utilização.

2.6.2. Características dos Roteadores

2.6.2.1. A CONTRATADA deverá fornecer pelo menos 2 (dois) roteadores, exclusivos, sendo um instalado nas dependências da CONTRATANTE e outro no ambiente de DATA CENTER da CONTRATADA;

2.6.2.2. O roteador deverá ser capaz de atender aos requisitos do link de comunicação de dados ponto-a-ponto entre a CONTRATANTE e o DATA CENTER da CONTRATADA;

2.6.2.3. Deve ser capaz de responder a pacotes de testes para avaliação da implementação dos níveis de serviço especificados. Devem ser suportados, no mínimo, os protocolos ICMP, TCP e UDP;

2.6.2.4. Cada roteador deverá possuir no mínimo 1 (uma) interface do tipo LAN padrão Gigabit Ethernet;

2.6.2.5. Cada roteador deverá operar com a taxa máxima de utilização de CPU e memória de até 80% (oitenta por cento).

2.6.2.6. As taxas máximas referentes ao roteador só serão levadas em consideração quando se mantiverem constantes em valores maiores ou iguais aos especificados por um período superior a 5 (cinco) minutos ou quando ocorrerem mais de 10 (dez) vezes ao longo de um único dia;

2.6.2.7. A operação dos roteadores com taxas superiores às especificadas neste item implicará na necessidade de sua substituição por outro equipamento, de maior capacidade, em até 30 (trinta) dias.

2.7. ITEM 6 – SERVIÇOS DE LINK DE INTERNET

2.7.1. Características Gerais

2.7.1.1. Deve ser fornecido 1 (um) link de internet dedicado para a conexão do ambiente de servidores contratados no DATA CENTER, conectando-o ao backbone da rede mundial de computadores, incluindo o fornecimento de equipamentos e a prestação de suporte técnico;

2.7.1.2. O serviço internet deverá ser disponibilizado pela CONTRATADA com a utilização de protocolo IP e concessão de um bloco de 10 (dez) endereços IP válidos e contínuos, correspondendo a um bloco CIDR/28;

2.7.1.3. Cada unidade deste item representa 1 (um) Mbps megabits por segundo de capacidade de conexão, sendo permitido à CONTRATADA ter a flexibilidade de contratar a quantidade de itens de 1Mbps, não inferior a 300 (trezentas) unidades, que irá definir a velocidade do link que deverá ser entregue pela CONTRATANTE;

2.7.1.4. Dentro do quantitativo de unidades de Mbps disponíveis, deve ser possível a flexibilidade de contratar mais de um link, com velocidade mínima de 100Mbps, podendo este ser instalado dentro do DATA CENTER contratado para prover alta disponibilidade de conexão ou em qualquer outra unidade da CONTRATANTE dentro da cidade de Palmas-TO, utilizando um número correspondente de unidades do item para cada Mbps contratado;

2.7.1.5. Todos os equipamentos/cabos devem ser homologados pela ANATEL.

2.7.1.6. A taxa de transmissão do canal deverá estar sempre disponível na totalidade do fluxo contratado no período;

2.7.1.7. A CONTRATADA deverá fornecer canal com transmissão full duplex e taxa simétrica, isto é, tenha a mesma capacidade de transmissão para o tráfego de entrada e de saída, simultaneamente;

2.7.1.8. Os canais de comunicação devem ser providos por meio de acessos terrestres via cabos ópticos;

2.7.1.9. Não será permitido o fornecimento de enlaces via satélite, nem a utilização de agregação de várias portas no roteador, pois a conexão deve ser fornecida utilizando uma única interface;

2.7.1.10. O canal e os roteadores deverão ser instalados na sala de equipamentos da CONTRATANTE;

2.7.1.11. A CONTRATADA deverá fornecer para a CONTRATANTE um meio on-line de consulta, com segurança de acesso, com informações de desempenho, latência, perda de pacote e ocupação do canal principal de comunicação ponto-a-ponto fornecido, gráficos de tendências e horários de maior e menor utilização;

2.7.1.12. A CONTRATADA deverá fornecer, dimensionar, disponibilizar, instalar, configurar, monitorar, operar, gerenciar e manter os equipamentos e recursos que forem necessários (roteadores, bastidores, meios de transmissão, cabeamento, dentre outros) para o provimento do serviço Internet da CONTRATANTE, especificado neste termo. Os equipamentos serão de propriedade da CONTRATADA que deverá ser responsável pelo suporte técnico dos mesmos, cumprindo com os tempos de atendimento estabelecidos neste termo.

2.7.2. Da Segurança

2.7.2.1. A CONTRATADA deve possuir central de monitoração do seu próprio Backbone, em regime 24x7 (serviço operacional e disponível 24 horas por dia, 7 dias por semana, todos os dias do ano), com objetivo de impedir ou limitar as chances de que ataques do tipo DOS (Denial of Service) e DDOS

(Distributed Denial of Service) atinjam o serviço de conexão à Internet objeto deste item. No caso de eventual ocorrência de ataque tipo DOS (Deny Of Service) e/ou DDOS (Distributed Deny Of Service), os filtros solicitados pela CONTRATANTE devem ser aplicados mediante solicitação.

2.7.3. Características dos Roteadores

2.7.3.1. A CONTRATADA deverá fornecer pelo menos 1 (um) roteador, exclusivo, sendo instalado nas dependências do DATA CENTER da CONTRATADA;

2.7.3.2. O roteador deverá ser capaz de atender aos requisitos do link de Internet contratado;

2.7.3.3. Deve ser capaz de responder a pacotes de testes para avaliação da implementação dos níveis de serviço especificados. Devem ser suportados, no mínimo, os protocolos ICMP, TCP e UDP;

2.7.3.4. Deverá possuir no mínimo 1 (uma) interface do tipo LAN padrão Gigabit Ethernet;

2.7.3.5. Deverá operar com a taxa máxima de utilização de CPU e memória de até 80% (oitenta por cento).

2.7.3.6. As taxas máximas referentes ao roteador só serão levadas em consideração quando se mantiverem constantes em valores maiores ou iguais aos especificados por um período superior a 5 (cinco) minutos ou quando ocorrerem mais de 10 (dez) vezes ao longo de um único dia;

2.7.3.7. A operação do roteador com taxas superiores às especificadas neste item implicará na necessidade de sua substituição por outro equipamento, de maior capacidade, em até 30 (trinta) dias;

2.7.3.8. A configuração lógica dos equipamentos CPE é de responsabilidade exclusiva da contratada, de maneira que atenda a todos os pré-requisitos e funcionalidades necessários ao correto funcionamento do link contratado.

2.7.3.9. Deverão ser non-blocking, com saída para a rede da contratada em porta ethernet 10Gbits/s;

2.7.3.10. Os roteadores deverão também atender aos seguintes requisitos mínimos:

2.7.3.11. Suportar capacidade de filtros de pacotes (por protocolo, endereço IP de origem, endereço IP de destino, porta de UDP/TCP de origem, porta de UDP/TCP de destino);

2.7.3.12. Suportar classificação de tráfego de acordo com diversos critérios (interface, IP origem/destino, portas TCP/UDP, MAC e serviço), em cada interface física e lógica (sub-interface);

2.7.3.13. Suporte a NAT (RFC1631) e suporte a VLANs (IEEE 802.1Q) com roteamento entre elas;

2.7.3.14. Suportar RFC791 (Internet Protocol).

2.8. ITEM 7 – SERVIÇOS DE LICENÇA WINDOWS SERVER 2022

2.8.1. Características Gerais

2.8.1.1. Deve ser fornecido 1 (uma) licença do Windows Server 2022 Standard, possibilitando alocação da mesma para a criação de instâncias de servidores virtuais;

2.8.1.2. As licenças devem ser válidas e estar em conformidade com os termos de licenciamento da Microsoft, devendo cada unidade desse item ser capaz de licenciar 1 (uma) instância de servidor virtual com até 1 (uma) vCPUs com Sistema Operacional Windows Server;

2.8.1.3. As licenças devem oferecer suporte adequado e atualizações de segurança contínuas.

2.9. ITEM 8 – SERVIÇOS GERENCIADOS DE FIREWALL

2.9.1. Características Gerais

2.9.1.1. A solução de Firewall será composta pelo fornecimento de um appliance virtual, bem como garantia e suporte técnico do fabricante pelo período de 12 (doze) meses;

2.9.1.2. Devem ser fornecidas todas as licenças necessárias para o funcionamento das funcionalidades de Filtro de Conteúdo Web, IPS, Gateway Antivírus, Controle de Aplicações e Proteção contra Ameaças Avançadas;

2.9.1.3. Toda Solução de segurança proposta deverá ser fornecida por um único fabricante de modo que tanto o suporte da solução quanto as funcionalidades de segurança sejam inteiramente integradas e gerenciadas através de uma única console de gerenciamento;

2.9.1.4. A solução deve consistir em plataforma de proteção de rede baseada em appliance virtual com funcionalidades de Next Generation Firewall. O termo Next Generation Firewall doravante será empregado como NGFW ou simplesmente FIREWALL;

2.9.1.5. O appliance deve suportar alocação de no mínimo 2vCPU e 8GB de memória RAM;

2.9.1.6. Deve suportar no mínimo 8 (oito) interfaces de rede multigiga (1G/10G) disponibilizada pelo Host;

2.9.1.7. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, prevenção de ataques zero-day, filtro de URL, identificação de usuários e controle granular de permissões;

2.9.1.8. Para proteção do ambiente contra-ataques, o dispositivo de proteção deve possuir módulos de IPS, Antivírus e Anti-Spyware (para bloqueio de arquivos maliciosos), integrados ao próprio appliance de NGFW;

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

2.9.1.10. Devem ser fornecidas todas as licenças necessárias para o funcionamento das funcionalidades de Filtro de Conteúdo Web, IPS, Gateway Antivírus, Controle de Aplicações e Proteção contra Ameaças Avançadas;

2.9.1.11. A solução deverá utilizar a tecnologia de firewall Stateful Packet Inspection com Deep Packet Inspection (suportar a inspeção da área de dados do pacote) para filtragem de tráfego IP;

2.9.1.12. As interfaces de rede do appliance deverão ser configuráveis pelo administrador do firewall para atender os segmentos de segurança e rede para:

2.9.1.12.1. Segmento WAN, ou externo;

2.9.1.12.2. Segmento WAN, secundário com possibilidade de ativação de recurso para redundância de WAN com balanceamento de carga e WAN Failover por aplicação. O equipamento deverá suportar no mínimo balanceamento de 4 links utilizando diferentes métricas pré-definidas pelo sistema;

2.9.1.12.3. Segmento LAN ou rede interna;

2.9.1.12.4. Segmento LAN ou rede interna podendo ser configurado como DMZ (Zona desmilitarizada)

2.9.1.12.5. Segmento LAN ou rede interna ou Porta de sincronismo para funcionamento em alta disponibilidade;

2.9.1.12.6. Segmento ou Zona dedicada para controle de dispositivos Wireless dedicado com controle e configuração destes dispositivos;

2.9.1.13. O appliance deve ter a capacidade de analisar tráfegos criptografados HTTPS/SSL/TSL onde o mesmo deverá ser descriptografado de forma transparente a aplicação, possibilitando a leitura de payload dos pacotes para checagem de assinaturas de aplicações conhecidas pelo fabricante, verificado possíveis ameaças e então re-criptografado e enviado juntamente ao seu destino caso este não contenha ameaças ou vulnerabilidades. O recurso poderá ser fornecido através de uma licença adicional ao appliance;

2.9.1.14. Controle, inspeção e de-criptografia de SSL/TLS por política para tráfego de entrada (Inbound) ou Saída (Outbound) com suporte a no mínimo, SSLv23, SSLv3, TLS 1.0, TLS 1.1, TLS 1.2 e TLS 1.3;

2.9.1.15. Não possuir limitação de segmentos de rede a serem protegidos;

2.9.1.16. Deve implementar mecanismo de sincronismo de horário através do protocolo NTP. Para tanto o appliance deve realizar a pesquisa em pelo menos 03 (três) servidores NTP distintos, com a configuração do tempo do intervalo de pesquisa;

2.9.1.17. Possibilitar o controle do tráfego para os protocolos TCP, UDP, ICMP e serviços como FTP, DNS, P2P entre outros, baseados nos endereços de origem e destino;

2.9.1.18. Deve permitir a utilização de regras de Anti-Vírus, Anti-Spyware, IPS e filtro de conteúdo web por segmentos de rede. Todos os serviços devem ser suportados no mesmo segmento de rede, VLAN ou zona de segurança.

2.9.1.19. Possuir flexibilidade para liberar aplicações da inspeção profunda de pacotes, ou seja, excluir a aplicação da checagem de IPS, Gateway Antivirus/Anti-Spyware;

2.9.1.20. Possibilitar o controle do tráfego para os protocolos GRE, H323 Full v1-5, suporte a tecnologia a gatekeeper, SIP e IGMP baseados nos endereços origem e destino da comunicação;

2.9.1.21. Controle e gerenciamento de banda para a tecnologia VoIP sobre diferentes segmentos de rede/segurança com inspeção profunda de segurança sobre este serviço;

2.9.1.22. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing) através da especificação da interface de rede pela qual uma comunicação deve se originar;

2.9.1.23. Prover mecanismos de proteção contra ataques baseados em “DNS Rebinding” protegendo contra códigos embutidos em páginas Web com base em JavaScript, Flash e base Java com “malwares”. O recurso deverá prevenir ataques e análises aos seguintes endereços:

2.9.1.23.1. Node-local address 127.0.0.1;

2.9.1.23.2. Link-local address 169.254.0.0/24;

2.9.1.23.3. Multicast address 224.0.0.0/24;

2.9.1.24. Host que pertence há alguma das sub-nets conectadas a: LAN, DMZ ou WLAN;

2.9.1.25. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem, subrede de origem e destino;

2.9.1.26. Possuir servidor de DHCP (Dynamic Host Configuration Protocol) interno com capacidade de alocação de endereçamento IP para as estações conectadas às interfaces do firewall e via VPN;

2.9.1.27. Deve suportar DHCP relay;

2.9.1.28. Prover a capacidade de encaminhamento de pacotes UDPs multicast/broadcast entre diferentes interfaces e zonas de segurança como IP Helper suportando os protocolos e portas:

2.9.1.28.1. Time service - UDP porta 37;

2.9.1.28.2. DNS - UDP porta 53;

2.9.1.28.3. DHCP - UDP portas 67 e 68;

2.9.1.28.4. Net-Bios DNS - UDP porta 137;

2.9.1.28.5. Net-Bios Datagram - UDP porta 138;

2.9.1.28.6. Wake On LAN - UDP porta 7 e 9;

2.9.1.28.7. mDNS - UDP porta 5353;

2.9.1.29. Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, SIP, RTP, RTSP e H323, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para acessos de dentro para fora quanto de fora para dentro;

2.9.1.30. A solução deve suportar funcionalidade de Geo-IP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade;

2.9.1.31. Possuir controle de número máximo de sessões TCP, prevenindo a exaustão de recursos do appliance e permitindo a definição de um percentual do número total de sessões disponíveis que podem ser utilizadas para uma determinada conexão definida por regra de acesso;

2.9.1.32. Possuir suporte ao protocolo SNMP versões 2 e 3;

2.9.1.33. Possuir suporte a log via syslog;

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

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

2.9.1.36. Deve suportar minimamente dois tipos de negação de tráfego nas políticas de firewall: Descarte sem notificação do bloqueio ao usuário (discard), descarte com notificação do bloqueio ao usuário (drop), descarte com opção de envio de “ICMP Unreachable” para máquina de origem do tráfego, “TCP-Reset” para o cliente, “TCP-Reset” para o servidor ou para os dois lados da conexão.

2.9.2. Características Anti-Malware:

2.9.2.1. Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado à plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream, permitindo o bloqueio de malwares (vírus, worms, spyware e etc);

2.9.2.2. Não serão permitidas soluções baseadas em redirecionamento de tráfego para dispositivos externos ao appliance para análise de arquivos ou pacotes de dados;

2.9.2.3. A atualização das assinaturas deverá ocorrer de forma automática sem há necessidade de intervenção humana;

2.9.2.4. Caso esta funcionalidade seja baseada em assinatura no formato subscrição, deverão ser fornecidas todas as licenças, sem custo adicional, pelo mesmo período solicitado pela garantia e suporte deste item;

2.9.3. Características IPS / IDS:

2.9.3.1. Possuir Mecanismo de IPS / IDS, baseado em assinatura, com suporte a pelo menos 3.000 (três mil) assinaturas de ataques, aplicações ou serviços, completamente integrados ao Firewall;

2.9.3.2. Não serão permitidas soluções baseadas em redirecionamento de tráfego para dispositivos externos ao appliance para análise de arquivos ou pacotes de dados;

2.9.3.3. O Sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes;

2.9.3.4. Possuir capacidade de remontagem de pacotes para identificação de ataques;

2.9.3.5. Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas à webserver para que seja usado para proteção específica de Servidores Web;

2.9.3.6. Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;

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

2.9.3.8. Detectar e bloquear a origem de portscans;

2.9.3.9. Reconhecimento de padrões;

2.9.3.10. Análise de protocolos;

2.9.3.11. Detecção de anomalias;

2.9.3.12. Detecção de ataques de RPC (Remote procedure call);

2.9.3.13. Proteção contra ataques DNS (Domain Name System);

2.9.3.14. Proteção contra ataques de ICMP (Internet Control Message Protocol);

2.9.3.15. Suportar reconhecimento de ataques de DDoS, reconnaissance, exploits e evasion;

2.9.3.16. A atualização das assinaturas deverá ocorrer de forma automática sem há necessidade de intervenção humana;

2.9.3.17. Caso esta funcionalidade seja baseada em assinatura no formato subscrição, deverão ser fornecidas todas as licenças, sem custo adicional, pelo mesmo período solicitado pela garantia e suporte deste item;

2.9.4. Filtro de Conteúdo Web:

2.9.4.1. Possuir módulo integrado ao mesmo NGFW para classificação de páginas web com no mínimo 50 (cinquenta) categorias distintas pré-definidas, com mecanismo de atualização e consulta automática;

2.9.4.2. Permitir a classificação dinâmica de sites web, URLs e domínios;

2.9.4.3. Das categorias pré-definidas, devem existir pelo menos as seguintes: violência, nudismo, roupas íntimas/banho, pornografia, armas, ódio / racismo, cultos / ocultismo, drogas / drogas ilegais, crimes / comportamento ilegal, educação sexual, jogos, álcool / tabagismo, conteúdo adulto, conteúdo questionável, artes e entretenimento, bancos / e-trading, chat, negócios e economia, tecnologia de computadores e Internet, e-mail pessoal, jogos de azar, hacking, humor, busca de empregos, newsgroups, encontros pessoais, restaurantes / jantar, portais de busca, shopping e portais de compras, MP3, download de software, viagens e WEB hosting;

2.9.4.4. Deve permitir a criação de no mínimo 5 (cinco) novas categorias personalizadas;

2.9.4.5. Possuir base contendo no mínimo 20 milhões de sites internet web já registrados e classificados com atualização automática;

2.9.4.6. Implementar filtro de conteúdo transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes;

2.9.4.7. Capacidade de submissão de novos sites através de portal web ou suporte do Fabricante;

2.9.4.8. Permitir a associação de grupos de usuários a diferentes regras de filtragem de sites web, definindo quais categorias deverão ser bloqueadas ou permitidas para cada grupo de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet;

2.9.4.9. Permitir a definição de quais zonas de segurança terão aplicadas as regras de filtragem de web;

2.9.4.10. O administrador poderá adicionar filtros por palavra-chave de modo específico;

2.9.4.11. Permitir aplicação da política de filtro de conteúdo baseada em horário do dia, bem como dia da semana;

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

2.9.4.13. Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente para o controle das políticas de Filtro de Conteúdo sem a necessidade de uma nova autenticação;

2.9.4.14. Permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies, activeX através de base de URL própria atualizável;

2.9.4.15. Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas, assim como, lista negra;

2.9.4.16. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem e por subrede de origem;

2.9.4.17. Deverá permitir o bloqueio Web através de senha pré configura pelo administrador;

2.9.4.18. Deverá permitir criar política de confirmação de acesso;

2.9.4.19. Deverá bloquear sites embarcados dentro outros sites como por exemplo translate.google.com.br;

2.9.4.20. Possibilitar a customização de mensagens de bloqueio para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança interna;

2.9.4.21. Caso esta funcionalidade seja baseada em assinatura no formato subscrição, deverão ser fornecidas todas as licenças para quantidade de usuários ilimitada, provendo atualização automática

e em tempo real através da categorização contínua de novos sites da Internet, sem custo adicional, pelo mesmo período solicitado pela garantia e suporte deste item.

2.9.5. Controle de aplicações:

2.9.5.1. Reconhecer no mínimo aplicações como: peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos e e-mail;

2.9.5.2. A solução deve possuir a capacidade de identificar pelo menos 1.500 (mil e quinhentas) aplicações para controle, bloqueio e agendamento deste recurso por usuário e grupo de usuário;

2.9.5.3. Possibilitar o controle sobre aplicações de forma granular com criação de políticas sobre o fluxo de dados de entrada, saída ou ambos e;

2.9.5.4. Devem ser aplicados por usuário e por grupo e;

2.9.5.5. Associado sua ação, políticas de horários e dias da semana e;

2.9.5.6. Podem ser associados a endereçamento IP baseados em sub-redes e;

2.9.5.7. Permitindo a restrição de arquivos por sua extensão e bloqueio de anexos através de protocolos SMTP e POP3 baseado em seus nomes ou tipos mime;

2.9.5.8. Permitir a filtragem de e-mails pelo seu conteúdo, através da definição de palavras-chave e a sua forma de pesquisa;

2.9.5.9. Prover matriz de horários que possibilite o bloqueio de serviços com granularidade baseada em hora, minutos, dia, dias da semana, mês e ano que a ação deverá ser tomada;

2.9.5.10. Controlar o uso dos serviços de Instant Messengers, de acordo com o perfil de cada usuário ou grupo de usuários, de modo a definir, para cada perfil, se ele pode ou não realizar download e/ou upload de arquivos, limitar as extensões dos arquivos que podem ser enviados/recebidos e permissões e bloqueio de sua utilização baseados em horários pré-determinados pelo administrador será obrigatório para este item;

2.9.5.11. Capacidade para realizar filtragens/inspeções dentro de portas TCP conhecidas por exemplo porta 80 HTTP, buscando por aplicações que potencialmente expõe o ambiente como: P2P, Kazaa, Morpheus, BitTorrent ou messengers;

2.9.5.12. Deverá controlar software FreeProxy tais como ToR, Ultrasurf, Freegate, dentre outros;

2.9.5.13. Caso esta funcionalidade seja baseada em assinatura no formato subscrição, deverão ser fornecidas todas as licenças, sem custo adicional, pelo mesmo período solicitado pela garantia e suporte deste item;

2.9.6. Proteção Contra Ameaças Avançadas:

2.9.6.1. A solução deverá prover as funcionalidades, através de serviço de sandbox local ou em nuvem, de inspeção de tráfego de entrada e saída de malwares não conhecidos (ameaças de dia zero) ou do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de callbacks;

2.9.6.2. Este mecanismo deve propiciar um ambiente isolado/controlado onde arquivos suspeitos ou aplicativos sejam executados, examinados e sondados antes que passem através do firewall para a rede interna;

2.9.6.3. Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador;

2.9.6.4. Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;

2.9.6.5. Suportar os protocolos HTTP assim como inspeção de tráfego criptografado através de HTTPS;

2.9.6.6. A solução deve ser capaz de inspecionar o tráfego criptografado SSL/TSL e SSH;

2.9.6.7. Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle;

2.9.6.8. Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN em tempo real;

2.9.6.9. O serviço deve suportar análise vários tipos e tamanhos de arquivos, incluindo programas executáveis, DLL, PDFs, ZIP, documentos do MS Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos, JAR e APK no ambiente controlado;

2.9.6.10. Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows e Android;

2.9.6.11. Deve possibilitar aos administradores personalizar a proteção, selecionando ou excluindo arquivos para serem enviados para a análise por tipo de arquivo, tamanho do arquivo, remetente, destinatário ou protocolo;

2.9.6.12. Deve possibilitar aos administradores enviarem arquivos manualmente para análise;

2.9.6.13. Para os arquivos enviados para o serviço avançado de proteção para análise, deve-se realizar o bloqueio de arquivos suspeitos até o veredicto, evitando que arquivos potencialmente maliciosos entrem na rede;

2.9.6.14. A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas;

2.9.6.15. Quando um arquivo for identificado como mal-intencionado, deve-se ser gerada uma assinatura imediatamente e disponibilizá-la para os firewalls, para evitar ataques subsequentes;

2.9.6.16. A atualização das assinaturas deverá ocorrer de forma automática sem há necessidade de intervenção humana;

2.9.6.17. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;

2.9.6.18. A análise em nuvem ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações, processos, registros são afetadas pelo malware, gerar assinaturas de Antivírus e Antispyware baseadas no hash da ameaça automaticamente, definir endereços e protocolos utilizados pela ameaça, mostrando a quantidade de dados trafegados nas conexões abertas pelo malware, a ferramenta deve prover e prover Informações sobre o usuário infectado (seu endereço IP ou seu login de rede);

2.9.6.19. Caso esta funcionalidade seja baseada em assinatura no formato subscrição, deverão ser fornecidas todas as licenças, sem custo adicional, pelo mesmo período solicitado pela garantia e suporte deste item;

2.9.7. Características de VPN:

2.9.7.1. Suportar a criação de túneis IP sobre IP (IPSEC Tunnel) de acordo com as RFCs 2401 a 2412, de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet, de modo a estabelecer canais de criptografia com outros produtos que também suportem tal padrão;

2.9.7.2. Implementar os esquemas de troca de chaves manual, IKE e IKEv2 por Pré-Shared Key, Certificados digitais e XAUTH client authentication;

2.9.7.3. Suportar os algoritmos de criptografia 3DES, AES 128 e AES 256;

2.9.7.4. Suportar os algoritmos Hash SHA-1, SHA-256 e SHA-384;

2.9.7.5. Diffie-Hellman: Grupo 2 (1024 bits), Grupo 5 (1536 bits) e Grupo 14 (2048 bits);

2.9.7.6. Suportar autenticação via de tuneis IPsec via certificado digital para VPNs Site-to-Site e Client-to-Site;

2.9.7.7. A solução deve suportar VPNs L2TP, incluindo suporte para Apple iOS e Android;

2.9.7.8. Solução deve suportar VPNs baseadas em políticas, e VPNs baseadas em roteamento estático e/ou dinâmico;

2.9.7.9. Solução deve incluir a capacidade de estabelecer VPNs com outros firewalls que utilizam IP públicos dinâmicos;

2.9.7.10. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do circuito primário;

2.9.7.11. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do primário;

2.9.7.12. Deve possuir interoperabilidade com pelo menos os seguintes fabricantes: Cisco, Check Point, Fortinet, Juniper, Palo Alto Networks e SonicWall.

2.9.8. Características de NAT:

2.9.8.1. Prover mecanismo de conversão de endereços (NAT), de forma a possibilitar que uma rede com endereços reservados acesse a Internet a partir de um único endereço IP e possibilitar também um mapeamento 1-1 de forma a permitir com que servidores internos com endereços reservados sejam acessados externamente através de endereços válidos;

2.9.8.2. Permitir, sobre o recurso de NAT, o balanceamento interno de servidores e suas aplicações sem a necessidade de inserção de um equipamento como switches de que atuam entre as camadas 4 (quatro) e 7 (sete) do modelo ISO/OSI.

2.9.8.3. Possuir mecanismo que permita que a conversão de endereços (NAT) seja feita de forma dependente do destino de uma comunicação, possibilitando que uma máquina, ou grupo de máquinas, tenham seus endereços convertidos para endereços diferentes de acordo com o endereço destino;

2.9.8.4. Possuir mecanismo que permita conversão de portas (PAT);

2.9.8.5. Implementar recurso de NAT (network address translation) tipo one-to-one, one-to-many, many-to-many, many-to-one, porta TCP de conexão (NAPT) e NAT Traversal em VPN IPsec (NAT-T) e NAT dentro do tunel IPsec.

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

2.9.9. Características de QoS:

2.9.9.1. Possuir gerenciamento de tráfego de entrada ou saída, por serviços, endereços IP e regra de firewall, permitindo definir banda mínima garantida e máxima permitida em porcentagem (%) para cada regra definida;

2.9.9.2. Permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (Shaping), criação de filas de prioridade e gerência de congestionamento;

2.9.9.3. Implementar 802.1p e classe de serviços CoS (Class of Service) de DSCP (Differentiated Services Code Points);

2.9.9.4. Permitir remarcação de pacotes utilizando TOS e/ou DSCP;

2.9.9.5. Limitar individualmente a banda utilizada por aplicação;

2.9.9.6. Deverá controlar (limitar) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;

2.9.9.7. Deverá controlar (limitar) individualmente a banda utilizada por subrede de origem e destino;

2.9.9.8. Deverá controlar (limitar) individualmente a banda utilizada por endereço IP de origem e destino.

2.9.10. Características de Roteamento:

2.9.10.1. Suportar os protocolos de roteamento RIP, RIPng, OSPF, OSPFv3 e BGP, sendo possível a configuração pela interface gráfica para, pelo menos, RIP, RIPng e OSPF;

2.9.10.2. Suportar Equal Cost Multi-Path (ECMP) no mínimo para roteamento estático e protocolo OSPF;

2.9.10.3. Suporte a Policy-Based Routing (PBR), com a capacidade de roteamento no mínimo, mas não limitado a: endereço de origem, endereço de destino, serviço e aplicação;

2.9.10.4. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC;

2.9.10.5. Permitir que seja criada políticas de roteamentos estáticos utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego sendo este visto pela regra de roteamento, como uma interface simples de rede para encaminhamento do tráfego;

2.9.10.6. Possibilitar o roteamento de tráfego IGMP versão 3 em suas interfaces e zonas de segurança.

2.9.11. Características de SD-WAN:

2.9.11.1. A solução deverá implementar tecnologia de SD-WAN (Software Defined WAN);

2.9.11.2. Capacidade de agregar no mínimo 4 (quatro) circuitos WAN distintos em um único canal lógico onde seja possível criar controles de caminho automático baseado em políticas, com habilidade de selecionar o melhor caminho, no mínimo, através dos seguintes parâmetros simultâneos: Latência, Jitter e Perda de pacotes.

2.9.11.3. O administrador da solução deverá ter a capacidade de configurar o canal lógico de SD-WAN para encaminhar tráfego simultaneamente por todos os links pertencentes a esse canal lógico;

2.9.11.4. A comutação do SD-WAN deve ocorrer de maneira dinâmica e automática baseada nas políticas previamente aplicadas;

2.9.11.5. A solução de SD-WAN deve permitir encaminhamento de tráfego com base em assinaturas de aplicações conhecidas (DPI), como Office 365, Facebook e Youtube, bem como aplicações associadas como Facebook Messenger e Office 365 Outlook.

2.9.12. Características de Gerenciamento Nativo:

2.9.12.1. Fornecer gerência remota, com interface gráfica WEB segura nativa, utilizando o protocolo HTTPS;

2.9.12.2. Possuir interface CLI (orientada a linha de comando) segura para a administração do firewall a partir do console com conexão via protocolo SSH;

2.9.12.3. A interface gráfica deverá possuir assistentes para facilitar a configuração inicial e a realização das tarefas mais comuns na administração do firewall, incluindo a configuração de VPN IPSECs, NAT, perfis de acesso e regras de filtragem;

2.9.12.4. Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o NGFW, cada um responsável por determinadas tarefas da administração;

2.9.12.5. Permitir a conexão simultânea de vários administradores, sendo um deles com poderes de alteração de configurações e os demais apenas de visualização das mesmas. Permitir que o segundo ao se conectar possa enviar uma mensagem ao primeiro através da interface de administração;

2.9.12.6. Possuir mecanismo que permita a realização de cópias de segurança (backups) e sua posterior restauração remotamente, através da interface gráfica;

2.9.12.7. Possuir mecanismo para realizar remotamente, através de interface gráfica, cópias de segurança (backup) e restauração de configurações e sistema operacional;

2.9.12.8. Possuir mecanismo para agendamento realização das cópias de segurança (backups) de configuração;

2.9.12.9. Possuir mecanismo para exportar as configurações através de FTP, HTTPs ou SFTP;

2.9.12.10. Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o NGFW remotamente através da interface gráfica;

2.9.12.11. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do NGFW, bem como possibilitar a remoção de qualquer uma destas sessões ou conexões;

2.9.12.12. Permitir a visualização, em tempo real, dos serviços com maior tráfego e os endereços IP mais acessados;

2.9.12.13. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas;

2.9.12.14. Permitir, através da interface gráfica remota, a visualização em forma gráfica e em tempo real das estatísticas do uso de CPU e tráfego de rede em todas as interfaces do NGFW;

2.9.12.15. A solução deve permitir ao administrador aplicar ajustes rápidos das melhores práticas de segurança no dispositivo com apenas um clique, possibilitando implementar as melhores práticas recomendadas pelo fabricante;

2.9.12.16. Ser capaz de visualizar, de forma direta no appliance e em tempo real estado do processamento do produto e volume/desempenho de dados utilizado pela rede de computadores conectada ao equipamento;

2.9.12.17. Possibilitar a geração de relatório de ameaças com avaliação e gerenciamento de riscos e informações detalhadas sobre o ambiente, ajudando a identificar explorações de vulnerabilidades, intrusões e outras ameaças. Deve permitir a emissão deste relatório em formato PDF;

2.9.12.18. Ser capaz de visualizar, de forma direta no appliance e em tempo real, a largura de banda utilizada por política, por protocolo TCP/UDP IPV4 e IPV6;

2.9.12.19. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as conexões estabelecidas, com possibilidade de aplicar filtros na visualização;

2.9.12.20. Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (considerando a existência do filtro de conteúdo Web);

2.9.12.21. Permitir habilitar auditoria de configurações no equipamento, possibilitando o rastreamento das configurações aplicadas no produto;

2.9.12.22. Ser capaz de implementar a funcionalidade de “Zero-Touch”, permitindo que o equipamento se provisione autônoma e automaticamente no sistema de gestão centralizada;

2.9.12.23. A solução deve possuir mecanismo de gerenciamento através de aplicativo móvel, com disponibilidade para os sistemas operacionais IOS e Android;

2.9.12.24. O aplicativo móvel deve possibilitar conexão ao dispositivo via protocolo HTTPS e conexão USB;

2.9.12.25. O gerenciamento via aplicativo móvel deve permitir visualização de status de consumo de banda, CPU, conexões ativas dos dispositivos e topologia do NGFW;

2.9.12.26. O aplicativo móvel deve permitir visualização de status das ameaças observadas e bloqueadas pelas funcionalidades de segurança de NGFW;

2.9.12.27. O aplicativo móvel deve permitir visualização dos últimos logs gerados no NGFW;

2.9.12.28. O aplicativo móvel deve permitir diagnósticos simples na solução, como testes ICMP e verificação DNS;

2.9.12.29. O aplicativo móvel deve permitir configurar interfaces, objetos e políticas de acesso, além de exportar configurações.

2.9.13. Características de Alta Disponibilidade:

2.9.13.1. Possuir mecanismo de Alta Disponibilidade operando em modo Ativo/Ativo ou Ativo/Passivo, com as implementações de Fail Over e Load Balance, sendo que na implementação de

Load Balance o estado das conexões e sessões TCP e UDP deve ser replicado sem restrições de serviços como, por exemplo, tráfego multicast;

2.9.13.2. Não serão permitidas soluções de cluster (HA) que façam com que os appliances reiniciem após qualquer modificação de parâmetro/configuração seja realizada pelo administrador;

2.9.13.3. A solução deve ter capacidade de fazer monitoramento físico das interfaces dos membros do cluster;

2.9.13.4. A solução deve operar em alta disponibilidade implementando monitoramento lógico de um host na rede, e possibilitar failover;

2.9.13.5. A solução deve permitir o uso de endereço MAC virtual para evitar problemas de expiração de tabela ARP em caso de Failover;

2.9.13.6. A solução deve possibilitar a sincronização de todas as configurações realizadas na caixa principal do cluster incluído, mas não limitado a objetos, regras, rotas, VPNs e políticas de segurança;

2.9.13.7. A solução deve permitir visualizar no equipamento principal, o status da comunicação entre os parceiros do cluster, status de sincronização das configurações, status atual do equipamento redundante;

2.9.13.8. O recurso de Alta Disponibilidade deverá ser suportado em modo Bridge;

2.9.14. Autenticação:

2.9.14.1. Prover autenticação de usuários para os serviços Telnet, FTP, HTTP e HTTPS, utilizando as bases de dados de usuários e grupos de servidores Windows e Unix, de forma simultânea;

2.9.14.2. Permitir a autenticação dos usuários utilizando servidores LDAP, AD, RADIUS, Tacacs+, Single Sign On e API;

2.9.14.3. Quando integrado com Microsoft Active Directory, deve reconhecer grupos de usuários cadastrados e prover funcionalidade de identificação transparente de usuários;

2.9.14.4. Permitir o cadastro manual dos usuários e grupos diretamente no NGFW por meio da interface de gerência remota do equipamento;

2.9.14.5. Permitir a integração com qualquer autoridade certificadora emissora de certificados X.509 que siga o padrão de PKI descrito na RFC 2459, inclusive verificando os certificados expirados/revogados, emitidos periodicamente pelas autoridades certificadoras, os quais devem ser obtidos automaticamente pelo NGFW;

2.9.14.6. Permitir o controle de acesso por usuário, para plataformas Microsoft Windows de forma transparente, para todos os serviços suportados, de forma que ao efetuar o login na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado sem a instalação de softwares adicionais nas estações de trabalho e sem configuração adicional no browser;

2.9.14.7. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no NGFW;

2.9.14.8. Permitir aos usuários o uso de seu perfil independentemente do endereço IP da máquina que o usuário esteja utilizando;

2.9.14.9. Permitir a atribuição de perfil por faixa de endereço IP nos casos em que a autenticação não seja requerida;

2.9.14.10. Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente através de regras no NGFW sem a necessidade de uma nova autenticação como por exemplo, para os serviços de navegação a Internet atuando assim de forma toda transparente ao usuário. Serviços como HTTP, HTTPS devem apenas consultar uma base de dados de usuários e grupos de servidores 2012/2016/2019 com AD.

2.9.15. Características de Capacidade e Performance:

2.9.15.1. A performance de Firewall SPI (Stateful Packet Inspection) deve ser de no mínimo 8 Gbps;

2.9.15.2. Deve suportar, em modo firewall, no mínimo 1.000.000 (um milhão) conexões concorrentes;

2.9.15.3. Deve suportar no mínimo 30.000 (trinta mil) novas conexões por segundo;

2.9.15.4. Performance de todos os serviços NGFW ativos (Gateway Antivírus, Anti-Spyware, IPS e Controle de Aplicativos) deverá ser de no mínimo 2.5 Gbps;

2.9.15.5. A performance de IPS deve ser de no mínimo 4 Gbps;

2.9.15.6. A performance mínima para a funcionalidade de análise de tráfegos criptografados HTTPS/SSL deverá ser de 1 Gbps;

2.9.15.7. A Performance de VPN IPSEC (3DES & AES 256) deverá ser de no mínimo 2 Gbps;

2.9.15.8. Deve suportar no mínimo 100 (cem) túneis VPN IPSEC do tipo site-to-site já licenciadas;

2.9.15.9. Deve suportar no mínimo 2.000 (dois mil) túneis VPN IPSEC do tipo client-to-site já licenciadas;

2.9.15.10. Suportar no mínimo 64 (sessenta e quatro) VLANs lógicas.

2.9.16. Módulo de Logs e Relatórios Analíticos:

2.9.16.1. A solução de NGFW a ser entregue, deverá possuir módulo de gerenciamento de logs e relatórios, podendo este ser ofertada em nuvem do próprio fabricante da solução de segurança ou em formato de appliance virtualizado;

2.9.16.2. Através do módulo de Gerenciamento de Logs e Relatórios deve ser possível coletar e armazenar fluxos e dados de log do NGFW e usá-los para análise de dados e relatórios analíticos;

2.9.16.3. Deve suportar o recebimento de logs dos equipamentos NGFW através do protocolo Syslog ou protocolo proprietário do fabricante, possibilitando o armazenamento de longo prazo de logs em uma única instância, ou seja, promover o recebimento e gerenciamento dos logs de vários appliances de forma centralizada;

2.9.16.4. Deve possuir Dashboard que indica informações sobre:

2.9.16.4.1. Aplicações e categorias de URL's mais acessadas;

2.9.16.4.2. Principais ameaças detectadas;

2.9.16.4.3. Número de vírus, intrusões, spyware, botnets, detectados;

2.9.16.4.4. Informações de conexões, tais como: total de conexões e taxa de conexões por segundo;

2.9.16.4.5. Informações sobre taxa de uso de banda e total de dados transferidos;

2.9.16.5. Deve possuir funcionalidade de relatórios sumarizados que forneçam um resumo executivo dos vários tipos de dados que estão sendo rastreados pelo NGFW, onde seja possível iniciar a verificação do funcionamento geral, bem como possuir relatórios detalhados;

2.9.16.6. Deve suportar a visualização e geração de no mínimo os seguintes relatórios:

2.9.16.6.1. Ameaças (vírus, spyware, botnets, intrusões, etc) que foram detectadas e bloqueadas;

2.9.16.6.2. Aplicativos, bem como a integridade dos mesmos, que passam pelo NGFW;

2.9.16.6.3. Usuários conectados ao sistema, onde seja possível identificar as transações e atividades a nível de usuário;

2.9.16.6.4. Acesso/conexões com base em categorias web, sendo possível realizar filtros por categoria;

2.9.16.6.5. Conexões com base no endereço IP e localidade de Origem/Destino;

2.9.16.7. Através da console deve ser possível verificar as atividades de navegação na Web de endereços IPs específicos, onde seja possível visualizar dados da sessão, tais como:

2.9.16.7.1. Data/hora de acesso;
2.9.16.7.2. Domínio e categoria da URL acessada
2.9.16.7.3. Endereço IP, Porta, MAC, Interface, Gateway e País do iniciador da conexão;

2.9.16.7.4. Informações sobre ameaça caso detectada;

2.9.16.7.5. Ação realizada pelo NGFW;

2.9.16.8. Deve possibilitar, através da console, monitorar: aplicações, usuários, atividades de navegação, Origens e Destinos de conexões, ameaças identificadas;

2.9.16.9. Deve suportar navegação “drill down” para realização de análise investigativas e obtenção de informações a rede, acesso do usuário, conectividade, uso de aplicativos, perfis de ameaças e outros dados relacionados ao NGFW.

2.9.16.10. Caso esta solução/funcionalidade seja baseada em assinatura no formato subscrição, deverão ser fornecidas todas as licenças, sem custo adicional, pelo mesmo período solicitado pela garantia e suporte deste item.

2.9.17. Outros Requisitos

2.9.17.1. O fabricante ou o produto deve possuir certificado ICSA (International Computer Security Association) para FIREWALL, ou CC (Common Criteria). Será aceito certificado equivalente ao ICSA, emitido por órgãos nacionais com competência para tal, desde que nos moldes deste, ou seja, certificado baseado na versão ou release atual do firewall, com manutenção recorrente deste certificado a cada mudança de versão, ou após determinado período de tempo, e baseado em normas nacionais e internacionais de segurança da informação;

2.9.17.2. Visando estabelecer efetividade de segurança dos firewalls de nova geração e assegurar que o fornecedor tenha uma solução já testada e comprovada por um órgão independente de mercado, o fabricante da solução deverá ser avaliado e certificado pelo NetSecOPEN, além de ser avaliado e citado pelo Gartner MQ (Magic Quadrant for Network Firewalls) nos relatórios de 2019 ou mais recentes;

2.9.17.3. O Fabricante deve comprovar participação no MAPP da Microsoft.

2.10. ITEM 9 – SERVIÇOS GERENCIADOS DE ANTIVÍRUS

2.10.1. Características Gerais:

2.10.1.1. A CONTRATADA deverá prover Serviços Gerenciados de Antivírus destinados à realização da proteção dos servidores, contemplando o monitoramento, gerenciamento e suporte;

2.10.1.2. Cada unidade deste item representa a proteção de uma instância de servidor, incluindo a licença do software de antivírus, bem como os serviços necessários para o monitoramento, gerenciamento e suporte;

2.10.1.3. O serviço deverá estar disponível em tempo integral, 24h por dia, 7 dias por semana;

2.10.1.4. Prestar todo o suporte técnico necessário para a perfeita execução do backup e/ou sua restauração e configuração;

2.10.1.5. Deverá ser utilizado software de antivírus profissional, atendendo todos os requisitos especificados no item “Características de Proteção e Recursos do Software Profissional de Antivírus”;

2.10.1.6. A CONTRATADA deve executar atividades de suporte proativo que devem compreender no mínimo:

2.10.1.6.1. Monitorar o console de gerenciamento: Verificar regularmente o console de gerenciamento da solução de antivírus para identificar quaisquer alertas, ameaças ou problemas de segurança. Ao identificar eventos de dispositivos que possuem um longo período desde a sua última conexão com a console de gerenciamento, novos dispositivos que foram descobertos na rede e não estejam protegidos pela solução de antivírus e também sobre

dispositivos que estiverem com status de proteção DESATIVADO/PAUSADO, deverá informar a equipe técnica da CONTRATANTE para que a mesma defina quais ações devem ser tomadas;

2.10.1.6.2. Verificar configuração e funcionamento da solução: Analisar periodicamente as configurações de políticas e tarefas, validando a correta execução das tarefas de administração agendadas, assim como analisar os resultados das mesmas, exemplo: (Verificações de malware, Atualizações de banco de dados, Backup das configurações da console de gerenciamento), além de identificar brechas e vulnerabilidades na configuração de regras implantadas e propor, de forma contínua, melhorias na proteção do ambiente, sempre que identificado a necessidade;

2.10.1.6.3. Verificar as atualizações de definições de vírus: Assegurar que as definições de vírus estejam atualizadas em todos os dispositivos. Verificar se as atualizações estão sendo baixadas e aplicadas corretamente;

2.10.1.6.4. Realizar varreduras completas do sistema: Agendar e executar varreduras completas em todos os dispositivos da rede para detectar e remover possíveis ameaças de malware;

2.10.1.6.5. Investigar e responder a alertas de ameaças: Analisar os relatórios e alertas gerados pela solução de antivírus, investigar possíveis ameaças, bem como comunicar a CONTRATANTE sobre os mesmos, cabendo a CONTRATANTE tomar as decisões para possíveis tratativas e mitigação dos riscos;

2.10.1.6.6. Gerenciar quarentena de arquivos suspeitos: Verificar regularmente a quarentena de arquivos da solução de antivírus para identificar possíveis falsos positivos ou arquivos maliciosos e tomar ações apropriadas, como a exclusão segura ou a restauração de arquivos legítimos;

2.10.1.6.7. Avaliar relatórios de segurança: Revisar os relatórios de segurança gerados pela solução de antivírus para identificar tendências, padrões de ameaças ou vulnerabilidades recorrentes. Utilizar essas informações para melhorar as políticas de segurança e tomar medidas preventivas adicionais;

2.10.1.6.8. Avaliar atualizações e patches de segurança de sistemas: executar tarefas para identificar vulnerabilidades conhecidas nos sistemas operacionais e aplicativos instalados, as quais que podem ser exploradas por atacantes, assim como fornecer a CONTRATANTE relatórios sobre as mesmas contendo fonte com informações sobre tal vulnerabilidade, cabendo a CONTRATANTE tomar as decisões para possíveis tratativas e mitigação dos riscos;

2.10.1.6.9. Realizar atualizações e patches: Garantir que todos os dispositivos estejam com a solução de antivírus atualizada com os patches de segurança mais recentes, informando previamente a CONTRATANTE sobre a implementação das mesmas;

2.10.1.6.10. Monitorar o desempenho da solução de antivírus: Verificar o desempenho da solução de antivírus, incluindo consumo de recursos, tempos de varredura e detecção de ameaças. Investigar e resolver quaisquer problemas de desempenho que possam afetar a eficácia ou a estabilidade do sistema;

2.10.1.6.11. Manter registros e documentação: Registrar e documentar todas as atividades relacionadas à gestão da solução de antivírus, incluindo ações tomadas, incidentes de segurança e soluções implementadas;

2.10.1.7. A CONTRATADA deve executar atividades de suporte reativo que devem compreender no mínimo:

2.10.1.7.1. Dúvidas técnicas sobre a configuração dos componentes de software que compõem o projeto, ou outras;

2.10.1.7.2. Criação e edição de regras na solução de gerenciamento, sejam elas pertinentes a exclusão de aplicativo/arquivo confiável, criação e edição de políticas de segurança, ou outras;

2.10.1.7.3. Restauração de arquivos excluídos pela solução de antivírus;

2.10.1.7.4. Restauração das configurações das soluções, quando houver necessidade;

2.10.1.7.5. Realizar análise e diagnóstico “troubleshooting”, no ambiente para resolução de problemas relacionados a solução de antivírus;

2.10.1.7.6. Abrir e acompanhar os chamados de suporte junto aos fabricantes das soluções, quando for o caso.

2.10.2. Características de Proteção e Recursos do Software Profissional de Antivírus

2.10.2.1. Servidor de Administração e Console de Gerenciamento

2.10.2.1.1. Deve possuir compatibilidade para instalação em Microsoft Windows Server 2019, 2022 Standard / Core / Datacenter x64;

2.10.2.1.2. A console deve ser acessada via WEB (HTTPS) ou MMC;

2.10.2.1.3. A console deve suportar arquitetura on-premise e arquitetura cloud-based;

2.10.2.1.4. Console deve ser baseada no modelo cliente/servidor;

2.10.2.1.5. A console deve suportar autenticação de dois fatores;

2.10.2.1.6. Deve possuir compatibilidade com Windows Failover Clustering;

2.10.2.1.7. O servidor de administração deve possuir modelo de cluster ativo-passivo;

2.10.2.1.8. Deve permitir a atribuição de perfis para os administradores da solução de Antivírus seguindo no mínimo os seguintes perfis pré-definidos:

2.10.2.1.8.1. Administrador;

2.10.2.1.8.2. Operador;

2.10.2.1.8.3. Supervisor;

2.10.2.1.9. Deve permitir incluir usuários do AD para logarem na console de administração;

2.10.2.1.10. Console deve ser totalmente integrada com suas funções e módulos, caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, gerenciamento de vulnerabilidades, detecção e resposta de endpoint, avaliação de vulnerabilidades, gerenciamento de dispositivos moveis;

2.10.2.1.11. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;

2.10.2.1.12. Deverá ser possível buscar novos produtos e soluções a partir da console;

2.10.2.1.13. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;

2.10.2.1.14. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, através da console de gerenciamento e GPO de AD.

2.10.2.1.15. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;

2.10.2.1.16. Deve armazenar histórico das alterações feitas em políticas;

2.10.2.1.17. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada;

2.10.2.1.18. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;

2.10.2.1.19. A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;

2.10.2.1.20. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;

2.10.2.1.21. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;

2.10.2.1.22. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário;

2.10.2.1.23. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;

2.10.2.1.24. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança;

2.10.2.1.25. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;

2.10.2.1.26. Capacidade de gerar pacotes customizados (auto-executáveis) contendo a licença e configurações do produto;

2.10.2.1.27. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;

2.10.2.1.28. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;

2.10.2.1.29. A comunicação entre o cliente e o servidor de administração deve ser criptografada;

2.10.2.1.30. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;

2.10.2.1.31. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

2.10.2.1.31.1. Nome do computador;

2.10.2.1.31.2. Nome do domínio;

2.10.2.1.31.3. Range de IP;

2.10.2.1.31.4. Sistema Operacional;

2.10.2.1.31.5. Máquina virtual.

2.10.2.1.32. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;

2.10.2.1.33. Deve ter a capacidade de descobrir novos dispositivos na rede, utilizando as seguintes técnicas:

2.10.2.1.33.1. Pesquisa de rede (Windows pooling);

2.10.2.1.33.2. Pesquisa ativa do AD (AD pooling);

2.10.2.1.33.3. Pesquisa de IP (IP pooling);

2.10.2.1.33.4. Pesquisa de rede (Zeroconf pooling);

2.10.2.1.34. Deve permitir, por meio da console de gerenciamento, extrair um artefato em área de backup de um cliente sem a necessidade de um servidor ou console de quarentena adicional;

2.10.2.1.35. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;

2.10.2.1.36. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção;

2.10.2.1.37. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;

2.10.2.1.38. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias, etc;

2.10.2.1.39. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;

2.10.2.1.40. Deve fornecer as seguintes informações dos computadores:

2.10.2.1.40.1. Se o antivírus está instalado;

2.10.2.1.40.2. Se o antivírus está iniciado;

2.10.2.1.40.3. Se o antivírus está atualizado;

2.10.2.1.40.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo;

2.10.2.1.40.5. Minutos/horas desde a última atualização de vacinas;

2.10.2.1.40.6. Data e horário da última verificação executada na máquina;

2.10.2.1.40.7. Versão do antivírus instalado na máquina;

2.10.2.1.40.8. Se é necessário reiniciar o computador para aplicar mudanças;

2.10.2.1.40.9. Quantidade de vírus encontrados (contador) na máquina;

2.10.2.1.40.10. Nome do computador;

2.10.2.1.40.11. Domínio ou grupo de trabalho do computador;

2.10.2.1.40.12. Data e horário da última atualização de vacinas;

2.10.2.1.40.13. Sistema operacional com Service Pack;

2.10.2.1.40.14. Quantidade de processadores;

2.10.2.1.40.15. Quantidade de memória RAM;

2.10.2.1.40.16. Sessões de usuários, com informações de contato (caso disponíveis no Active Directory);

2.10.2.1.40.17. Endereço IP;

2.10.2.1.40.18. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;

2.10.2.1.40.19. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD e placa mãe;

2.10.2.1.40.20. Vulnerabilidades de aplicativos instalados na máquina;

2.10.2.1.41. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;

2.10.2.1.42. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

2.10.2.1.42.1. Alteração de Gateway Padrão;

2.10.2.1.42.2. Alteração de subrede;

2.10.2.1.42.3. Alteração de domínio;

2.10.2.1.42.4. Alteração de servidor DHCP;

2.10.2.1.42.5. Alteração de servidor DNS;

- 2.10.2.1.42.6.** Alteração de servidor WINS;
- 2.10.2.1.42.7.** Resolução de Nome;
- 2.10.2.1.42.8.** Disponibilidade de endereço de conexão SSL;
- 2.10.2.1.43.** Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
- 2.10.2.1.44.** Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
- 2.10.2.1.45.** Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
- 2.10.2.1.46.** A console de gerenciamento deve suportar funções de controle de acesso com base na função (RBAC) para a hierarquia de servidores;
- 2.10.2.1.47.** Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
- 2.10.2.1.48.** Capacidade de herança de configuração de tarefas, políticas e relatórios na estrutura de hierarquia de servidores on-premisse com servidor em cloud;
- 2.10.2.1.49.** Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;
- 2.10.2.1.50.** Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;
- 2.10.2.1.51.** Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;
- 2.10.2.1.52.** Capacidade de monitoramento do sistema através de um SNMP client;
- 2.10.2.1.53.** Capacidade enviar eventos através de protocolo de syslog;
- 2.10.2.1.54.** Capacidade exportar eventos para sistemas de SIEM no formato LEEF e CEF;
- 2.10.2.1.55.** Deve ser capaz de enviar os eventos para sistemas de SIEM em canal encriptado;
- 2.10.2.1.56.** Dever ter a capacidade de exportar eventos para sistemas de SIEM, compatível com Qradar, ArcSight e Splunk;
- 2.10.2.1.57.** Capacidade de enviar e-mails para contas específicas em caso de algum evento;
- 2.10.2.1.58.** Listar em um único local, todos os computadores não gerenciados na rede;
- 2.10.2.1.59.** Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes;
- 2.10.2.1.60.** Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente;
- 2.10.2.1.61.** Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação etc.), inclusive de máquinas que estejam em subnets diferentes do servidor;
- 2.10.2.1.62.** Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);

2.10.2.1.63. Deve através de opções de otimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo, porém sem comprometer o desempenho do computador;

2.10.2.1.64. Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (ex: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint);

2.10.2.1.65. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros;

2.10.2.1.66. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

2.10.2.1.67. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

2.10.2.1.67.1. Nome do vírus;

2.10.2.1.67.2. Nome do arquivo infectado;

2.10.2.1.67.3. Data e hora da detecção;

2.10.2.1.67.4. Nome da máquina ou endereço IP;

2.10.2.1.67.5. Ação realizada.

2.10.2.1.68. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;

2.10.2.1.69. Capacidade de listar updates nas máquinas com o respectivo link para download;

2.10.2.1.70. Deve criar um backup de todos os arquivos deletados em computadores durante a desinfecção para que possam ser restaurados;

2.10.2.1.71. Deve ter uma área de backup na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante;

2.10.2.1.72. Capacidade de realizar resumo de hardware de cada máquina cliente;

2.10.2.1.73. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

2.10.2.2. Recursos e proteções do Antivírus para Estações de Trabalho Windows Virtuais.

2.10.2.2.1. Deve ser compatível com os seguintes sistemas de estação de trabalho Microsoft Windows 10 Pro e 11Pro / Enterprise / Home / Education;

2.10.2.2.2. Apesar da Licença solicitada no item 7 seja de Windows Server, a necessidade de compatibilidade com os sistemas operacionais citados acima é necessária, pois o ambiente de cloud computing a ser contratado será utilizado não apenas para hospedar servidores, mas também para criar máquinas virtuais (VMs) que simulem estações de trabalho com os sistemas operacionais citados.

2.10.2.2.3. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

2.10.2.2.4. Antivírus de Web (módulo para verificação de sites e downloads contra vírus);

2.10.2.2.5. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);

2.10.2.2.6. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável;

2.10.2.2.7. Deve possuir módulo dedicado contra prevenção de intrusão, Prevenção de intrusão do host;

2.10.2.2.8. Autoproteção (contra-ataques aos serviços/processos do antivírus);

2.10.2.2.9. Controle de dispositivos externos;

2.10.2.2.10. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc;

2.10.2.2.11. Controle de acesso a sites por horário;

2.10.2.2.12. Controle de acesso a sites por usuários;

2.10.2.2.13. Controle de acesso a websites por dados, ex: Bloquear websites com conteúdo de vídeo e áudio;

2.10.2.2.14. Controle de execução de aplicativos;

2.10.2.2.15. Controle de vulnerabilidades do Windows e dos aplicativos instalados;

2.10.2.2.16. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

2.10.2.2.17. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);

2.10.2.2.18. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

2.10.2.2.19. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação;

2.10.2.2.20. Capacidade de adicionar aplicativos a uma lista de “aplicativos confiáveis”, onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;

2.10.2.2.21. Deverá possuir módulo dedicado para proteção contra port scanning;

2.10.2.2.22. Deverá possuir módulo dedicado para proteção contra network flooding;

2.10.2.2.23. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);

2.10.2.2.24. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

2.10.2.2.25. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

2.10.2.2.26. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;

2.10.2.2.27. Deverá possuir módulo para proteção contra malwares que tenta realizar criptografia de arquivos em pastas compartilhadas.

2.10.2.2.28. Deve ter a capacidade de detectar ameaças instaladas na BIOS ROM do endpoint.

2.10.2.2.29. Deverá realizar scanner de firmware em busca de rootkits.

2.10.2.2.30. Ao detectar uma ameaça, a solução deve exibir informações: do objeto SHA256 e/ou do objeto MD5;

2.10.2.2.31. Capacidade de verificar somente arquivos novos e alterados;

2.10.2.2.32. Capacidade de verificar objetos usando heurística;

2.10.2.2.33. Capacidade de agendar uma pausa na verificação de arquivos;

2.10.2.2.34. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;

2.10.2.2.35. Capacidade de pausar automaticamente a verificação de arquivos quando um aplicativo for iniciado;

2.10.2.2.36. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

2.10.2.2.36.1.1. Perguntar o que fazer, ou;

- 2.10.2.2.36.1.2.** Bloquear acesso ao objeto;
- 2.10.2.2.36.1.3.** Apagar o objeto ou tentar desinfecção-lo (de acordo com a configuração pré-estabelecida pelo administrador);
- 2.10.2.2.36.1.4.** Caso positivo de desinfecção: Restaurar o objeto para uso;
- 2.10.2.2.36.1.5.** Caso negativo de desinfecção: Mover para uma área de backup ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
- 2.10.2.2.37.** Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
- 2.10.2.2.38.** Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, IMAP, NNTP, SMTP, MAPI;
- 2.10.2.2.39.** Capacidade de verificar links inseridos em e-mails contra phishings;
- 2.10.2.2.40.** Capacidade de verificar todo o tráfego web de acessos à internet nos protocolos HTTP, HTTPS e FTP, utilizando técnicas de banco de dados, serviços da nuvem do fabricante e análise de heurística bloqueado arquivos, sites de phishing e URL maliciosas;
- 2.10.2.2.41.** Capacidade de verificação de corpo e anexos de e-mails usando heurística;
- 2.10.2.2.42.** O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:
 - 2.10.2.2.42.1.** Perguntar o que fazer, ou;
 - 2.10.2.2.42.2.** Bloquear o e-mail;
 - 2.10.2.2.42.3.** Apagar o objeto ou tentar desinfecção-lo (de acordo com a configuração pré-estabelecida pelo administrador);
 - 2.10.2.2.42.4.** Caso positivo de desinfecção: Restaurar o e-mail para o usuário;
 - 2.10.2.2.42.5.** Caso negativo de desinfecção: Mover para uma área de backup ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);
- 2.10.2.2.43.** Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;
- 2.10.2.2.44.** Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;
- 2.10.2.2.45.** Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script etc);
- 2.10.2.2.46.** Deve ser possível realizar o monitoramento das atividades de rede em tempo real, visualizando portas UDP/TCP e Tráfego de rede por aplicativo.
- 2.10.2.2.47.** Capacidade de alterar as portas monitoradas pelos módulos de ameaças web, controle de acesso à web e e-mail;
- 2.10.2.2.48.** Na verificação de tráfego web, caso encontrado código malicioso o programa deve: Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio;
- 2.10.2.2.49.** O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:
 - 2.10.2.2.49.1.** Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo real;
 - 2.10.2.2.49.2.** Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação;
- 2.10.2.2.50.** Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;
- 2.10.2.2.51.** Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências

características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;

2.10.2.2.52. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas;

2.10.2.2.53. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (<http://www.antiphishing.org/>);

2.10.2.2.54. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;

2.10.2.2.55. Deve possuir módulo para proteção contra port scans, network flooding e MAC spoofing. A base de dados de análise deve ser atualizada juntamente com as vacinas;

2.10.2.2.56. Deve permitir a importação e exportação de listas de regras e exclusões para as aplicações no formato XML;

2.10.2.2.57. Deve permitir a criação de zonas confiáveis locais independentes por parte do usuário.

2.10.2.2.58. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

2.10.2.2.58.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

2.10.2.2.58.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

2.10.2.2.59. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:

2.10.2.2.59.1. Discos de armazenamento locais;

2.10.2.2.59.2. Armazenamento removível;

2.10.2.2.59.3. Impressoras;

2.10.2.2.59.4. CD/DVD;

2.10.2.2.59.5. Drives de disquete;

2.10.2.2.59.6. Modems;

2.10.2.2.59.7. Dispositivos de fita;

2.10.2.2.59.8. Dispositivos multifuncionais;

2.10.2.2.59.9. Leitores de smart card;

2.10.2.2.59.10. Wi-Fi;

2.10.2.2.59.11. Adaptadores de rede externos;

2.10.2.2.59.12. Dispositivos MP3 ou smartphones;

2.10.2.2.59.13. Dispositivos Bluetooth;

2.10.2.2.59.14. Câmeras e Scanners.

2.10.2.2.60. Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário;

2.10.2.2.61. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;

2.10.2.2.62. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;

2.10.2.2.63. Deve permitir controlar o acesso a dispositivos externos com base em prioridade de regras.

2.10.2.2.64. Capacidade de habilitar “logging” em dispositivos removíveis tais como Pendrive, Discos externos etc.

2.10.2.2.65. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;

2.10.2.2.66. Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto etc.);

2.10.2.2.67. Ter a capacidade de detectar a modificação de firmware em dispositivos USB mal-intencionado.

2.10.2.2.68. Deverá realizar a validação dos dispositivos que se conectam via USB que emulam teclados;

2.10.2.2.69. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:

2.10.2.2.69.1. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.

2.10.2.2.69.2. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.

2.10.2.2.70. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

2.10.2.2.71. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo;

2.10.2.2.72. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web;

2.10.2.2.73. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

2.10.2.2.74. Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware.

2.10.2.2.75. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.

2.10.2.2.76. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

2.10.2.2.77. Capacidade de integração com a Antimalware Scan Interface (AMSI).

2.10.2.2.78. Deve permitir realizar o gerenciamento por meio de integração via REST API.

2.10.2.2.79. Deve permitir o gerenciamento remoto da solução por meio de aplicativos de administração remota.

2.10.2.3. Recursos e proteções do Antivírus para Servidores Windows

2.10.2.3.1. Deve ser compatível com os seguintes sistemas operacionais:

2.10.2.3.1.1. Windows Server 2016 Essentials / Standard / Datacenter;

2.10.2.3.1.2. Windows Server 2019 Essentials / Standard / Datacenter;

2.10.2.3.1.3. Windows Server 2022.

2.10.2.3.2. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

2.10.2.3.3. Auto-proteção contra-ataques aos serviços/processos do antivírus;

2.10.2.3.4. Firewall com IDS;

- 2.10.2.3.5.** Controle de vulnerabilidades do Windows e dos aplicativos instalados;
- 2.10.2.3.6.** Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- 2.10.2.3.7.** Deve permitir gerenciamento, no mínimo, das seguintes formas:
- 2.10.2.3.7.1.** Via console administrativa;
- 2.10.2.3.7.2.** Via web (remotamente);
- 2.10.2.3.8.** As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
- 2.10.2.3.9.** Deverá ter a capacidade de customizar o uso de CPU para realização de scanner no dispositivo.
- 2.10.2.3.10.** O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
- 2.10.2.3.10.1.** Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
- 2.10.2.3.10.2.** Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados;
- 2.10.2.3.11.** Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total;
- 2.10.2.3.12.** Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede;
- 2.10.2.3.13.** Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros etc.);
- 2.10.2.3.14.** Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;
- 2.10.2.3.15.** Deve possuir funcionalidade de análise personalizada de logs do Windows;
- 2.10.2.3.16.** Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;
- 2.10.2.3.17.** Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;
- 2.10.2.3.18.** Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;
- 2.10.2.3.19.** Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
- 2.10.2.3.20.** Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação;
- 2.10.2.3.21.** Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
- 2.10.2.3.22.** Capacidade de verificar somente arquivos novos e alterados;
- 2.10.2.3.23.** Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);
- 2.10.2.3.24.** Capacidade de verificar objetos usando heurística;
- 2.10.2.3.25.** Capacidade de configurar diferentes ações para diferentes tipos de ameaças;

2.10.2.3.26. Capacidade de agendar uma pausa na verificação;

2.10.2.3.27. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

2.10.2.3.27.1. Bloquear acesso ao objeto;

2.10.2.3.27.2. Apagar o objeto ou tentar desinfecção (de acordo com a configuração pré-estabelecida pelo administrador);

2.10.2.3.27.3. Caso positivo de desinfecção: Restaurar o objeto para uso;

2.10.2.3.27.4. Caso negativo de desinfecção: Mover para área de backup ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

2.10.2.3.28. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

2.10.2.3.29. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos maliciosos em área de backup;

2.10.2.3.30. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

2.10.2.3.31. Em caso de detecção de sinais de uma infecção ativa, deve possuir capacidade de, automaticamente:

2.10.2.3.31.1. Executar os procedimentos pré-configurados pelo administrador;

2.10.2.3.31.2. Em caso de ausência de procedimentos pré-configurados, criar tais procedimentos e executá-los;

2.10.2.3.32. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

2.10.2.3.33. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros;

2.10.2.3.34. Capacidade de detectar anomalias no comportamento de um software usando análise heurística;

2.10.2.3.35. Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta;

2.10.2.3.36. Deve possuir controle de dispositivos externos.

2.10.2.4. Recurso de Gerenciamento de Sistemas

2.10.2.4.1. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;

2.10.2.4.2. Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários;

2.10.2.4.3. Capacidade de atualizar informações sobre hardware presentes nos relatórios após mudanças de hardware nas máquinas gerenciadas;

2.10.2.4.4. Capacidade de gerenciar um inventário de hardware;

2.10.2.4.5. Possibilita fazer distribuição de software de forma manual e agendada;

2.10.2.4.6. Suporta modo de instalação silenciosa;

2.10.2.4.7. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;

2.10.2.4.8. Possibilita fazer a distribuição através de agentes de atualização;

2.10.2.4.9. Utiliza tecnologia multicast para evitar tráfego na rede;

2.10.2.4.10. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;

2.10.2.4.11. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;

2.10.2.4.12. Capacidade de gerar relatórios de vulnerabilidades e patches;

2.10.2.4.13. Possibilitar a seleção para aplicação de patch por dispositivo gerenciado ou grupo de administração;

2.10.2.4.14. Permitir reiniciar ou não o endpoint durante a instalação de patch e correções de vulnerabilidades;

2.10.2.4.15. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;

2.10.2.4.16. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;

2.10.2.4.17. Permite selecionar produtos a serem atualizados pela console de gerenciamento;

2.10.2.4.18. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc;

2.10.2.4.19. Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;

2.10.2.4.20. Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;

2.10.2.4.21. Capacidade de configurar o reinício do computador após a aplicação das atualizações e correções de vulnerabilidades;

2.10.2.4.22. Deve permitir selecionar o idioma das aplicações que serão atualizadas;

2.10.2.4.23. Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes;

2.10.2.5. Detecção e Resposta (Endpoint Detection and Response)

2.10.2.5.1.1. Deve ser compatível com os seguintes sistemas operacionais:

2.10.2.5.1.1.1. Microsoft Windows 10 Pro;

2.10.2.5.1.1.2. Microsoft Windows 11 Pro;

2.10.2.5.1.1.3. Windows Server 2016 Standard / Datacenter;

2.10.2.5.1.1.4. Windows Server 2019 Standard / Datacenter;

2.10.2.5.1.1.5. Windows Server 2022 Standard / Datacenter;

2.10.2.6. Características:

2.10.2.6.1.1. As funcionalidades relacionadas a detecção e resposta solicitadas nesse item, devem ser operadas na mesma console de gerenciamento da solução de endpoint;

2.10.2.6.1.2. A solução deve oferecer módulo focado em capacidades de EDR “Endpoint Detection and Response”, incluindo no mínimo as seguintes capacidades:

2.10.2.6.1.3. O agente deve ter capacidade de coletar e processar dados relacionadas ao veredito e ao contexto da ameaça;

2.10.2.6.1.4. Deve fornecer graficamente a visualização da cadeia do ataque;

2.10.2.6.1.5. Deve possuir a capacidade de varredura, para identificar a presença de um artefato detectado em outros dispositivos na rede, através de indicadores de comprometimento (IoC).

2.10.2.6.1.6. A varredura deve oferecer opções de resposta automatizada (sem intervenção do administrador), para serem executadas caso o IoC seja encontrado em outro dispositivo, com no mínimo as seguintes opções:

2.10.2.6.1.6.1. Isolar o host;

2.10.2.6.1.6.2. Iniciar uma varredura;

2.10.2.6.1.6.3. Quarentenar o objeto;

2.10.2.6.1.7. A solução deve criar um report detalhado sobre o incidente, tendo a capacidade de incluir no mínimo os seguintes dados:

2.10.2.6.1.7.1. Visibilidade das detecções provenientes de endpoint;

2.10.2.6.1.7.2. Processos;

2.10.2.6.1.7.3. Conexões remotas;

2.10.2.6.1.7.4. Alterações de registros;

2.10.2.6.1.7.5. Objetos baixados;

2.10.2.6.1.8. Capacidade de integração com a solução de sandbox cloud do fabricante;

2.10.2.6.1.9. Varredura por todos os dispositivos executada a partir de indicador de comprometimento (IoC) gerado através da solução e importado pelo administrador.

2.10.2.6.1.10. Deverá possuir informações de assinaturas digitais da ameaça;

2.10.2.6.1.11. Deve ser capaz de trazer informações do arquivo sobre sua geolocalização;

2.10.2.6.1.12. Possibilidade de informar quando o arquivo foi detectado pela base de conhecimento;

2.10.2.6.1.13. Trazer a identificação de comportamento e/ou descrição sobre o arquivo;

2.10.2.6.1.14. A solução deve oferecer no mínimo as seguintes opções de resposta:

2.10.2.6.1.14.1. Prevenir a execução de um arquivo;

2.10.2.6.1.14.2. Quarentenar um arquivo;

2.10.2.6.1.14.3. Iniciar uma varredura por IoC;

2.10.2.6.1.14.4. Parar um processo;

2.10.2.6.1.14.5. Executar um processo;

2.10.2.6.1.15. Ferramenta que possibilite o isolamento do host infectado com no mínimo as características abaixo:

2.10.2.6.1.16. A opção de isolamento deve estar disponível junto a visualização do incidente;

2.10.2.6.1.17. Na análise do incidente a ferramenta deverá apresentar recomendações de ações que o analista precisa executar para remediar o incidente;

2.10.2.6.1.18. Deverá ser possível remover a máquina do isolamento a partir do incidente;

2.10.2.6.1.19. Na configuração padrão, o isolamento deve ser feito de forma granular, permitindo o controle do dispositivo pela console administrativa mesmo após ativação da regra;

2.10.2.6.1.20. Deve oferecer informações de inteligência de ameaças do próprio fabricante;

2.10.2.6.1.21. Deverá possuir detecção baseada em sandbox do tipo cloud;

2.10.2.6.1.22. Deverá suportar IoC de terceiros em formatos OpenIOC;

2.11. ITEM 10 – SERVIÇOS GERENCIADOS DE BACKUP

2.11.1. Características Gerais:

2.11.1.1. A CONTRATADA deverá prover Serviços Gerenciados de Backup em nuvem destinados à realização da proteção, armazenamento e recuperação de dados dos servidores, contemplando o monitoramento, gerenciamento e suporte;

2.11.1.2. Realizar via solução profissional de backup especificada a proteção (backup) completa (sistema operacional, aplicativos instalados, configurações e dados), diário e/ou intervalos pré-determinados, automaticamente, dos servidores críticos elencados pela CONTRATANTE;

2.11.1.3. Cada unidade deste item representa a proteção de uma instância de servidor, incluindo a licença do software de backup, bem como os serviços necessários para o monitoramento, gerenciamento e suporte do backup;

2.11.1.4. Para a área de armazenamento necessária para o repositório do backup, será realizado a contratação do item “SERVIÇOS DE ARMAZENAMENTO EM BLOCO (HDD)” adicional ao volume necessário deste item que será alocado para a instâncias de servidores;

2.11.1.5. Deverá possibilitar configuração de política de backup para realizar snapshots com frequências diárias, semanais e a cada intervalo de horas, podendo essa frequência ser customizável para cada servidor protegido, conforme interesse da CONTRATANTE;

2.11.1.6. Deverá reter os dados protegidos pelo período mínimo de 30 (trinta) dias sem sobrescrevê-los, e o espaço necessário para o repositório de backup e para esta retenção deverá ser considerado e limitado em 25% do volume alocado para a instância de servidor protegido;

2.11.1.7. Prestar todo o suporte técnico necessário para a perfeita execução do backup e/ou sua restauração e configuração;

2.11.1.8. Realizar a recuperação (restauração) dos dados (da base de dados completa ou apenas arquivos específicos) sempre que demandado pelo CONTRATANTE e sem custos adicionais;

2.11.1.9. Trafegar os dados do backup sempre de forma segura, utilizando padrões de criptografia;

2.11.1.10. A CONTRATADA deverá informar onde o serviço será prestado, ou seja, o endereço dos servidores de backup, obrigatoriamente localizado em território nacional;

2.11.1.11. O sistema deve funcionar em ambiente privado e os arquivos salvos devem possuir uma cópia local no Data Center da CONTRATADA e o outra replicada em uma outra nuvem sob sua gestão;

2.11.1.12. O serviço deverá estar disponível em tempo integral, 24h por dia, 7 dias por semana;

2.11.1.13. Ao final do contrato, todos os dados deverão ser apagados dos repositórios de Backup, sem possibilidade de recuperação, utilizando DELEÇÃO por “ZERO FILL” garantindo a integridade SIGILOSA do serviço;

2.11.1.14. Deverá ser utilizado software de backup profissional, atendendo todos os requisitos especificados no item “Características de Proteção e Recursos do Software Profissional de Backup”;

2.11.2. Serviços de Gerenciamento, Monitoramento e Suporte:

2.11.2.1. A CONTRATADA deverá prover serviços de gerenciamento, monitoramento e suporte, prestados remotamente por meio Centro de Operação de Segurança;

2.11.2.2. Gerenciar e monitorar o backup diário de dados, alertando em casos de falhas, pouco espaço em disco ou erros de qualquer natureza e propor e/ou realizar a imediata correção;

2.11.2.3. Realizar a análise do ambiente atual da CONTRATANTE (identificando modo de operação) e efetuar ajustes no ambiente de backup, caso necessário;

2.11.2.4. Prestar todo o suporte técnico necessário para a perfeita execução do backup e/ou sua restauração e configuração;

2.11.2.5. Realizar a recuperação (restauração) dos dados (da base de dados completa ou apenas arquivos específicos) sempre que demandado pela COTRATANTE e sem custos adicionais;

2.11.2.6. Os serviços de monitoramento remoto deverão ser realizados pela CONTRATADA, na modalidade 24h por dia, 7 dias por semana.

2.11.2.7. A CONTRATADA deverá disponibilizar, mensalmente, até o 5º dia útil do mês posterior à prestação de serviços, através de e-mail ou via impressa, os seguintes relatórios de utilização dos últimos 30 (trinta) dias:

2.11.2.7.1. Status de trabalhos bem-sucedidos, trabalhos com falha e trabalhos com erros;

2.11.2.7.2. Máquinas protegidas, máquinas replicadas e pontos de restauração disponíveis;

2.11.2.7.3. Status do repositório, contendo volume consumido e volume livre;

2.11.2.8. Os serviços de suporte técnico devem contemplar as seguintes ações e/ou premissas:

2.11.2.8.1. Recepcionar via telefone ou e-mail, e registrar corretamente à abertura de qualquer chamado técnico referente à solução;

2.11.2.8.2. Implantar e manter scripts de atendimento adequados às necessidades de suporte técnico da CONTRATANTE;

2.11.2.8.3. Implantar e manter base de conhecimento adequada às necessidades de suporte técnico da CONTRATANTE;

2.11.2.8.4. Solucionar problemas ou sanar dúvidas por telefone e/ou e-mail quanto aos questionamentos repassados pela CONTRATANTE;

2.11.2.8.5. Acionar equipes específicas da CONTRATADA para realizar a reposição antecipada de equipamentos defeituosos, quando for necessário;

2.11.2.8.6. Notificar e encaminhar para a CONTRATANTE, nova atualização de softwares e firmwares dos produtos ofertados, quando disponibilizado pelo fabricante, bem como o respectivo procedimento de atualização;

2.11.2.8.7. Agendar visitas de manutenção corretiva com a CONTRATANTE, registrando chamados para este fim;

2.11.2.8.8. Acompanhar os chamados desde sua abertura até seu encerramento, independente de existir ou não redirecionamento para outras equipes técnicas da própria CONTRATADA ou FABRICANTE;

2.11.2.8.9. Elaboração e emissão de relatórios executivos mensais contendo as atividades realizadas e o resumo dos dados em aberto;

2.11.2.9. Os serviços de suporte técnico devem estar disponíveis em horário comercial durante sua vigência, ou seja, de segunda a sexta-feira das 8 às 18h exceto feriados;

2.11.2.10. Para os serviços de suporte técnico, a CONTRATADA deverá possuir Central de Atendimento, disponibilizando contato por telefone, e-mail e ferramenta web para abertura e acompanhamento dos chamados em regime 24x7, ou seja, de segunda a domingo, das 00:00h às 23:59h.

2.11.2.11. Caberá à Central de Atendimento, ser o contato único entre a CONTRATADA e a CONTRATANTE, registrando todas as solicitações e registros de ocorrência em sistema eletrônico específico para estes fins, além de fornecer à CONTRATANTE o número de identificação da ocorrência para acompanhamento.

2.11.3. Características de Proteção e Recursos do Software Profissional de Backup

2.11.3.1. Deve possuir capacidade de efetuar backups, através de políticas pré-definidas e agendadas;

2.11.3.2. Deve possuir uma central de controle unificada para gerenciar operações de backup, recuperação e replicação em todas as plataformas compatíveis (virtuais, físicas, em nuvem);

2.11.3.3. Deve possuir autenticação de múltiplos fatores (MFA) para usuários administradores garantindo uma camada adicional de segurança no acesso ao sistema;

2.11.3.4. Deve ser plenamente compatível com a autenticação Kerberos;

2.11.3.5. Deve fornecer funcionalidades de geolocalização para a gestão de dispositivos que estão sob a proteção do serviço de backup;

2.11.3.6. Deve proporcionar suporte para a criação de contas de usuário com privilégios administrativos, destinadas ao controle, gerenciamento e monitoramento das operações relacionadas aos serviços de backup. Deve ser possível criar, no mínimo, as seguintes categorias de usuários:

2.11.3.6.1. Administrador;

2.11.3.6.2. Operador;

2.11.3.6.3. Visualizador;

2.11.3.7. Deve suportar Backup de máquinas virtuais Amazon EC e Microsoft Azure Virtual Machines;

2.11.3.8. Deve ser possível a criação de um cache de backup local temporário, para que computadores que não possuam conexão ao local de backup remoto possam salvar os dados em um cache local e posteriormente ao estabelecer sua devida conexão salvar os dados no repositório de backup remoto;

2.11.3.9. Deve ser capaz de suportar certificados TLS a fim de estabelecer uma conexão segura para serviços de backup;

2.11.3.10. Deve ser possível a criação de grupos destinados a proteção e gerência dos dispositivos;

2.11.3.11. Deverá garantir, no mínimo, a proteção de máquinas virtuais e seus dados, gerenciadas através das soluções de virtualização VMware ou Hyper-V;

2.11.3.12. Suportar servidores proxy de backup virtuais ou físicos para backup de máquinas virtuais;

2.11.3.13. Deve oferecer recursos que possibilitam a ordenação de atividades e trabalhos de backup com base em prioridades automaticamente definidas;

2.11.3.14. Deve incluir detalhes sobre os objetos de backup, incorporando pelo menos as seguintes informações:

2.11.3.14.1. Quantidade de pontos de restauração disponíveis;

2.11.3.14.2. Data de criação dos pontos de restauração;

2.11.3.14.3. Dimensão do backup;

2.11.3.15. O software de backup deve realizar a proteção dos dados no conceito de snapshots podendo configurar o intervalo de tempo entre a geração dos mesmos, contendo intervalos periódicos mínimos a cada uma hora;

2.11.3.16. Deve ser possível a restauração de arquivos e pastas individuais;

2.11.3.17. Deverá assegurar a consistência de aplicações transacionais de forma automática por meio da integração com Microsoft VSS, dentro de sistemas operacionais Windows;

2.11.3.18. Deve ser possível realizar a reinicialização do computador ou servidor protegido através da console de gerenciamento;

2.11.3.19. Deverá possuir recursos de replicação de máquinas virtuais no ambiente VMware vSphere, possibilitando a criação de cópias precisas em formato nativo para rápida recuperação em caso de desastre;

2.11.3.20. Permitir a criação de backups incrementais, ou seja, uma vez que foi feito o primeiro backup completo, os subsequentes devem ser sempre incrementais;

2.11.3.21. Deverá oferecer a possibilidade de armazenar os arquivos de backup de forma criptografada, com algoritmo mínimo de 256 bits, ativando e desativando tal operação, assim como

assegurar o trânsito da informação através desse cenário, mesmo que impacte a performance da gravação;

2.11.3.22. Deve incluir funcionalidades de imutabilidade a fim de assegurar a segurança dos dados de backup;

2.11.3.23. Deve possuir recursos para realizar a verificação de integridade dos backups de VMs;

2.11.3.24. Fornecer opções para administrar as operações de backup, incluindo a capacidade de pausar e retomar uma tarefa de backup;

2.11.3.25. Deverá oferecer trabalhos de cópia de backup com implementação de políticas de retenção;

2.11.3.26. Deve permitir a modificação das políticas de backup conforme necessário, o que inclui a capacidade de alterar o escopo, o local de destino dos backups e os horários de execução;

2.11.3.27. Capacidades para conduzir testes de validação de backups, assegurando a restauração segura, incluindo a detecção de malware a partir de um motor de varredura (Antivírus) da própria solução ou de terceiros;

2.11.3.28. Quanto às funcionalidades de deduplicação, deverá minimamente; suportar deduplicação de blocos na origem (client side), de forma que o cliente envie apenas novos blocos de dados criados e/ou modificados a partir do último backup, além disso deve suportar deduplicação de dados nos servidores de mídia (destino), de forma que o mesmo descarte blocos repetidos enviados pelos clientes, evitando assim o armazenamento de blocos redundantes;

2.11.3.29. Deve ser capaz de oferecer suporte a repositórios de backup, garantindo compatibilidade com as seguintes configurações:

2.11.3.29.1. Servidores Diretamente Anexados: Windows Server e Linux;

2.11.3.29.2. Armazenamento de Rede Anexado: SMB (Server Message Block) e NFS (Network File System);

2.11.3.30. Deve suportar repositórios em nuvem, possuindo suporte aos seguintes provedores de nuvem:

2.11.3.30.1. Azure

2.11.3.30.2. Amazon

2.11.3.30.3. GCP;

2.11.3.31. A solução deve possuir agente compatíveis com ambientes Windows:

2.11.3.31.1. Windows 8.1;

2.11.3.31.2. Windows 10;

2.11.3.31.3. Windows Server 2008 R2;

2.11.3.31.4. Windows Server 2012;

2.11.3.31.5. Windows Server 2012 R2;

2.11.3.31.6. Windows Server 2016;

2.11.3.31.7. Windows Server 2019;

2.11.3.31.8. Windows Server 2022;

2.11.3.32. A solução deve possuir agente compatíveis com ambientes Linux:

2.11.3.32.1. Red Hat Enterprise Linux (RHEL) 6.4 ou superior;

2.11.3.32.2. CentOS 7;

2.11.3.32.3. Oracle Linux 6 ou superior;

2.11.3.32.4. Debian Linux 10.13 ou superior;

2.11.3.32.5. Ubuntu 16.04 ou superior;

2.11.3.32.6. SuSE Linux Enterprise Server 12 SP4;

2.11.3.33. Deverá garantir a recuperação granular e consistente, sem necessidade de agentes adicionais para o ambiente virtualizado através das soluções, principalmente para os seguintes softwares:

2.11.3.33.1. Microsoft Active Directory 2008 a 2022;

2.11.3.33.2. Microsoft Exchange Server 2013 a 2019;

2.11.3.33.3. Microsoft SQL Server 2008 a 2022;

2.11.3.33.4. Microsoft Sharepoint 2013 a 2019;

2.11.3.33.5. Oracle Database 11g a 21c;

2.12. ITEM 11 – SERVIÇOS NOC

2.12.1. Características Gerais

2.12.1.1. O NOC deve ser planejado pela CONTRATADA em conformidade com as melhores práticas de gerenciamento de serviços de TIC;

2.12.1.2. O NOC deve estar disponível em regime integral de 24 (vinte e quatro) horas x 7 (sete) dias na semana e em feriados;

2.12.1.3. O NOC deverá operar remotamente;

2.12.1.4. A equipe de colaboradores que operam no NOC deve ser capacitada tecnicamente e dimensionada pela CONTRATADA de modo a atender todos os requisitos técnicos deste Termo de Referência;

2.12.1.4.1. Cada unidade deste item representa o monitoramento de até 10 (dez) ativos, ou seja, a cada unidade que for contratada a CONTRATADA deverá monitorar até 10 (dez) ativos. Entende-se como ativo: servidores físicos/virtuais, roteadores, switches, firewalls, links de dados, aplicações e serviços, dentre outros dispositivos de rede passíveis de monitoramento remoto.

2.12.2. Atividades do NOC

2.12.2.1. Executar rotinas e procedimentos técnicos diários de modo a prevenir/detectar incidentes/problemas no ambiente tecnológico de TIC da CONTRATANTE de forma proativa;

2.12.2.2. Manter os softwares que compõem a solução sempre com informações atualizadas e fidedignas do ambiente tecnológico de TIC da CONTRATANTE;

2.12.2.3. Promover o Gerenciamento de Incidentes e Problemas, realizando a comunicação, identificação, tratamento, resolução e/ou escalonamentos de todos os alertas oriundos do ambiente tecnológico de TIC da CONTRATANTE, integrando as equipes necessárias pelo atendimento;

2.12.2.4. Realizar a abertura de chamado junto às empresas contratadas pela CONTRATANTE em caso de indisponibilidade e/ou degradação do ambiente tecnológico da CONTRATANTE, integrando as equipes necessárias pelo atendimento;

2.12.2.5. Apresentar relatórios gerais oriundos dos sistemas que compõem a solução em qualquer tempo e sempre que solicitado pela CONTRATANTE.

2.12.3. Serviços Gerenciados de Monitoramento de Ambiente Tecnológico - NOC:

2.12.3.1. Composição dos serviços gerenciados de monitoramento de ambiente tecnológico:

2.12.3.1.1. Monitoramento de Rede;

2.12.3.1.2. Monitoramento de Servidores;

2.12.3.1.3. Monitoramento de Máquina Virtual;

2.12.3.1.4. Monitoramento de Aplicações/Serviços;

2.12.3.2. O monitoramento deverá ser de forma ininterrupta, 24x7;

2.12.3.3. A ferramenta será fornecida pela CONTRATADA e será disponibilizado para acesso do corpo técnico da CONTRATANTE;

2.12.3.4. O Gerenciamento administrativo, bem como a abrangência de itens de configuração alvo da ferramenta de monitoramento do parque tecnológico será de responsabilidade da CONTRATANTE;

2.12.3.5. A CONTRATADA deverá disponibilizar APP para acesso ao monitoramento.

2.12.4. Central de Atendimento

2.12.4.1. Deverá ser disponibilizado um Canal de Atendimento em regime integral de 24 (vinte e quatro) horas em 7 (sete) dias na semana e em feriados;

2.12.4.2. O Canal de Atendimento deverá ser implementado por meio de ferramentas de comunicação disponibilizadas pela CONTRATADA de modo a garantir a disponibilidade de contato, sendo, no mínimo:

2.12.4.2.1. Via plataforma Microsoft Teams;

2.12.4.2.2. Via aplicativo WhatsApp;

2.12.4.2.3. Via E-mail;

2.12.4.2.4. Via telefone, com a disponibilização de 2 (dois) números de contato;

2.12.4.3. Outros canais de comunicação poderão ser também disponibilizados pela CONTRATADA, desde que com a anuência da CONTRATANTE e sem prejuízo ao regime de atendimento especificado neste Termo de Referência.

2.13. ITEM 12 – SERVIÇOS TÉCNICOS ESPECIALIZADOS E CONTINUADOS

2.13.1. Características Gerais

2.13.1.1. Será realizado como prestação de serviço, continuado e sob demanda, com banco de horas;

2.13.1.2. O saldo do banco de horas terá validade de 12 meses, sendo descontado e pago mensalmente o valor correspondente às horas usadas do banco;

2.13.1.3. O serviço poderá ser realizado remotamente (através de software próprio da CONTRATADA) ou presencialmente, conforme necessidade para a solução da requisição/incidente;

2.13.1.4. A CONTRATANTE poderá exigir, no ato de abertura do incidente ou requisição, dependendo do nível de criticidade do atendimento, que o atendimento seja feito de maneira presencial ou de maneira remota;

2.13.1.5. O atendimento deverá ser realizado por profissionais que possuam experiência comprovada para o atendimento completo das soluções;

2.13.1.6. A CONTRATANTE poderá a qualquer momento solicitar a substituição imediata dos técnicos envolvidos no atendimento caso julgue ineficiente os resultados inerentes à prestação de serviço e resolução dos problemas. Nestes casos, a CONTRATADA terá um prazo de até 48 (quarenta e oito) horas úteis para a substituição da equipe de atuação;

2.13.1.7. A solicitação do serviço será feita pelo CONTRATANTE, através de chamado (eletrônico ou telefônico), e-mail ou documento oficial, expedido ao prestador;

2.13.1.8. O período de abertura e resolução dos chamados será contabilizado no regime 8x5 (8 horas e 5 dias da semana);

2.13.1.9. A CONTRATADA deverá dispor de telefone em DDD (63) ou número 0800 ou permitir ligações à cobrar para a abertura de chamados;

2.13.1.10. A CONTRATADA deverá disponibilizar e-mail para a abertura de chamados;

2.13.1.11. A CONTRATADA deverá dispor de software próprio para registro e controle dos

chamados, com registro de hora e data do evento, descrição do caso relatado, técnico responsável pelo atendimento, histórico e continuidade da solicitação e emissão de estatísticas e relatórios fixos ou sob demanda;

2.13.1.12. Para controle e aprovação da utilização do banco de horas, juntamente com a nota fiscal dos serviços faturada mensalmente, é necessário a apresentação de relatório mensal com o resumo das horas gastas, bem como a relação completa de atividades/chamados e o tempo de atendimento específico de cada um deles;

2.13.1.13. As atividades que compreendem o atendimento serão:

2.13.1.13.1. Análise, planejamento e migração dos servidores e sistemas hospedados no ambiente da CONTRATANTE para o ambiente de Data Center da CONTRATADA;

2.13.1.13.2. Suporte durante todo o processo de migração e testes completos de funcionalidade pós-migração;

2.13.1.13.3. Dúvidas técnicas sobre a configuração dos componentes que compõem o projeto, ou outras;

2.13.1.13.4. Alterações nas políticas de configuração do ambiente virtual;

2.13.1.13.5. Criação de máquinas virtuais;

2.13.1.13.6. Instalação, configuração de sistemas operacionais Windows Server e Linux, contemplando as distribuições Ubuntu, CentOS, Red Hat, bem como o diagnóstico e resolução de problemas nos mesmos;

2.13.1.13.7. Configuração e solução de problemas relacionados a redes (TCP/IP, DNS, DHCP) no ambiente Windows e Linux;

2.13.1.13.8. Configuração e suporte de serviços de servidor, como Apache (servidor web), MySQL/MariaDB (banco de dados), SSH, FTP, IIS (Internet Information Services), SQL Server, Exchange Server, entre outros;

2.13.1.13.9. Automação de tarefas por meio de scripts, utilizando ferramentas como Shell Script, Python, etc;

2.13.1.13.10. Resolução de problemas de desempenho, diagnóstico de falhas e otimização do sistema operacional;

2.13.1.13.11. Implementação e gerenciamento de atualizações de patches de segurança e service packs;

2.13.1.13.12. Abrir e acompanhar os chamados de suporte junto aos fabricantes das soluções, quando for o caso.

3. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO (Anexo III, Art. 6º, Inciso III do Decreto 552/24)

3.1.A ASSEMBLEIA LEGISLATIVA DO TOCANTINS - ALETO, atualmente conta com uma estrutura on-premises, aonde a mesma está totalmente desatualizada com mais de 15 anos de defasagem e equipamentos totalmente fora de garantia e sem suporte de fabricante.

3.2.A ALETO está sempre em busca das melhores práticas de mercado e das tecnologias mais atuais dessa forma estando em constante evolução tecnológica para oferecer a nossa instituição o que há de melhor a fim de oferecer sempre um serviço de qualidade e alto valor agregado.

3.3. Além disso, a ALETO também busca aplicar as boas práticas estabelecidas pela transformação digital que todo o mundo está passando, intensificando as suas ações de modernização de processos operacionais, de modo a reduzir a burocracia e aumentar a sua eficiência, aumentando assim a quantidade e qualidade dos serviços ofertados.

3.4. Neste contexto, este projeto busca intensificar o uso de tecnologias que estejam em uma infraestrutura robusta de armazenamento e processamento de dados de modo a otimizar os custos de infraestrutura e serviços de TI, possibilitando assim, mitigar possíveis riscos, danos ou indisponibilidade à prestação dos serviços de TI, decorrentes de problemas técnicos identificados nos equipamentos atualmente utilizados nesta casa de Leis.

3.5. Diante do que foi mencionado sobre o cenário atual da infraestrutura de tecnologia da informação de que dispomos, fica evidente a necessidade da modernização do Datacenter atualmente em uso, o que permitirá à Assembleia Legislativa do Estado do Tocantins contar com a expertise e conhecimentos técnicos necessários para implementar e gerenciar uma solução eficiente.

4. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERANDO O CICLO DE VIDA DO OBJETO (Anexo III, Art. 6º Inciso II, do Decreto 552/24)

4.1. A solução de TIC a ser Contratada consiste em contratar servidores virtuais, nesse caso, uma empresa especializada para implantação e execução de serviços em nuvem que represente provedores em nuvem.

4.2. A ALETO pode armazenar seus dados de forma segura em sua nuvem privada, enquanto utiliza o seu Data Center físico para hospedar outros serviços. Essa combinação garante a segurança dos dados confidenciais e permite que a ALETO ofereça serviços inovadores e eficientes à população do Tocantins.

4.3. Em suma, a arquitetura de servidores de forma híbrida oferece a ALETO a combinação ideal de segurança, conformidade, otimização de custos, escalabilidade, agilidade, inovação e melhor gestão de TI, tornando-se a escolha ideal para modernizar sua infraestrutura e aprimorar a prestação de serviços aos servidores, Deputados e conseqüentemente à comunidade.

4.4. Esta solução se destina a atender requisitos técnicos de contingenciamento de serviços essenciais sustentados pela ALETO, para possibilitar hospedagem em IaaS (Infrastructure as a Service), com o intuito de maximizar a disponibilidade dos serviços, sem degradar os outros conceitos de segurança da informação, confidencialidade e integridade. O provedor de serviços de computação em nuvem deverá possuir aderência a padrões de conformidade, confidencialidade e segurança mínimos com aderência as normas/certificações: ABNT NBR.

4.5. Serviços de VCPU

4.5.1. Uma VCPU, ou virtual CPU, é uma unidade de processamento virtual que representa um núcleo de processamento em um servidor físico. Em ambientes de computação em nuvem, os provedores de serviços alocam vCPUs para máquinas virtuais (VMs), permitindo que usuários e organizações executem aplicações e serviços sem a necessidade de comprar e gerenciar hardware físico.

4.6. Serviços de memória RAM

4.6.1. Os serviços em nuvem que oferecem memória RAM (Random Access Memory) são essenciais para o desempenho de aplicações e serviços em ambientes de computação em nuvem. A memória RAM é um componente crítico que permite que as máquinas virtuais (VMs) e os aplicativos acessem dados e instruções rapidamente, melhorando a eficiência e a velocidade de processamento. A memória RAM em um ambiente de nuvem refere-se à quantidade de memória

volátil alocada para máquinas virtuais (VMs) ou contêineres que estão sendo executados em servidores físicos de um provedor de nuvem. A RAM é utilizada para armazenar dados temporários e instruções que são necessárias para a execução de aplicações em tempo real.

4.7. Serviços de armazenamento em bloco NVMe (GB)

4.7.1. Os serviços em nuvem de armazenamento em bloco NVMe (Non-Volatile Memory Express) são uma solução moderna e de alto desempenho para armazenar e gerenciar dados em ambientes de computação em nuvem. O armazenamento em bloco é especialmente adequado para aplicações que exigem acesso rápido e frequente a dados, como bancos de dados, sistemas de arquivos e aplicações empresariais críticas.

4.7.2. O armazenamento em bloco NVMe refere-se a uma tecnologia de armazenamento que utiliza a interface NVMe para conectar unidades de estado sólido (SSDs) a servidores. Essa tecnologia é projetada para maximizar a velocidade e a eficiência no acesso a dados, aproveitando a alta largura de banda e baixa latência oferecidas pelos SSDs.

4.8. Serviços de armazenamento em bloco HDD (GB)

4.8.1. Os serviços em nuvem de armazenamento em bloco HDD (Hard Disk Drive) são uma solução de armazenamento que utiliza discos rígidos tradicionais para gerenciar e armazenar dados em ambientes de computação em nuvem. Esse tipo de armazenamento é frequentemente utilizado para aplicações que não exigem alta performance, mas que ainda precisam de uma solução confiável e econômica para armazenar grandes volumes de dados.

4.9. Serviços de link LAN-TO-LAN

4.9.1. O serviço LAN-TO-LAN permite que redes locais em diferentes locais físicos sejam conectadas de forma segura e eficiente, como se estivessem em uma única rede local. Isso é feito através da utilização de conexões diretas através de provedores de serviços em nuvem.

4.10. Link de Internet

4.10.1. O link de internet é uma conexão que permite que dispositivos e redes se conectem à internet. Em um contexto de serviços em nuvem, isso pode incluir a provisão de acesso à internet para usuários finais, bem como a conectividade entre recursos em nuvem e a infraestrutura local de uma organização.

4.11. Serviços de licenças WINDOWS SERVER

4.11.1. O Windows Server é um sistema operacional desenvolvido pela Microsoft, projetado especificamente para servidores e ambientes corporativos. Ele oferece uma variedade de serviços e funcionalidades, incluindo gerenciamento de rede, armazenamento, virtualização, e serviços de aplicação, tornando-se uma escolha popular para empresas de todos os tamanhos.

4.12. Serviços gerenciados de FIREWALL

4.12.1. Os serviços gerenciados de firewall em nuvem são soluções de segurança que protegem redes e aplicações contra ameaças cibernéticas, controlando o tráfego de entrada e saída com base em políticas de segurança definidas. Esses serviços são essenciais para garantir a integridade, confidencialidade e disponibilidade dos dados e sistemas em ambientes de nuvem.

4.12.2. Esse serviço é uma solução de segurança que fornece proteção em tempo real contra ameaças cibernéticas, como malware, ataques de negação de serviço (DDoS), e tentativas de acesso não autorizado. Esses serviços são gerenciados por provedores de segurança, que configuram, monitoram e mantêm as políticas de firewall, permitindo que as organizações se concentrem em suas atividades principais.

4.13. Serviços gerenciados de ANTIVÍRUS

4.13.1. Um serviço gerenciado de antivírus é uma solução de segurança que fornece proteção contínua contra malware e outras ameaças cibernéticas, utilizando tecnologia de nuvem para monitorar e proteger sistemas e dispositivos. Esses serviços incluem não apenas a detecção e remoção de vírus, mas também a prevenção de infecções e a resposta a incidentes de segurança.

4.14.Serviços gerenciados de BACKUP

4.14.1. Os serviços gerenciados de backup são soluções que permitem a cópia e a proteção de dados armazenados em servidores, dispositivos e aplicações. Esses serviços utilizam a nuvem para armazenar backups, garantindo que os dados estejam seguros e acessíveis em caso de incidentes, como falhas de hardware, ataques cibernéticos ou desastres naturais.

4.15.Serviços de NOC (pct 10 ativos)

4.15.1. Os serviços de NOC é composto por um Centro de Operações de Rede (NOC) que é uma instalação centralizada onde as equipes de TI monitoram e gerenciam a infraestrutura de rede de uma organização. Os serviços NOC incluem a supervisão de redes, servidores e aplicações, bem como a identificação e resolução de problemas técnicos. Com a migração para a nuvem, muitas organizações optam por serviços NOC gerenciados que operam em ambientes de nuvem.

4.16.Serviços Técnicos Especializados

4.16.1. Os serviços técnicos especializados de horas em nuvem, referem-se a soluções que oferecem suporte técnico e consultoria por meio de profissionais qualificados, cobrados com base no tempo de serviço prestado. Esses serviços são projetados para atender a necessidades específicas de tecnologia da informação (TI) e podem incluir uma ampla gama de atividades, como implementação, configuração, manutenção e suporte de sistemas e aplicações. A seguir, está uma descrição detalhada sobre os serviços técnicos especializados em horas em nuvem.

4.17. Ciclo de Vida da Contratação

4.17.1. Planejamento da Contratação

4.17.1.1. Levantamento de Necessidades: Definição da demanda, requisitos técnicos e objetivos da contratação.

4.17.1.2. Análise de Viabilidade: Avaliação de soluções disponíveis no mercado e viabilidade técnica, econômica e jurídica.

4.17.1.3. Elaboração do Estudo Técnico Preliminar (ETP): Justificativa da necessidade e estimativa de custos.

4.17.1.4. Construção do Termo de Referência (TR): Definição do objeto, requisitos técnicos, nível de serviço esperado, métricas de desempenho e responsabilidades das partes.

4.17.2. Seleção e Contratação do Fornecedor

4.17.2.1. Definição da Modalidade de Contratação: Licitação, dispensa ou adesão a ata de registro de preços, conforme normativos aplicáveis.

4.17.2.2. Publicação do Edital e Recebimento de Propostas: Análise técnica e financeira das propostas.

4.17.2.3. Julgamento e Homologação: Escolha do fornecedor conforme critérios estabelecidos.

4.17.2.4. Assinatura do Contrato ou Termo de Adesão: Formalização da contratação com cláusulas de penalidade e governança.

4.17.3. Implementação e Gestão do Contrato

4.17.3.1. Provisionamento dos Serviços: Ativação do ambiente e configuração inicial conforme os requisitos do TR.

4.17.3.2. Monitoramento e Gestão: Acompanhamento da entrega do serviço, métricas de SLA (tempo de resposta, disponibilidade, desempenho), e conformidade com requisitos de segurança e governança.

4.17.3.3. Fiscalização do Contrato: Execução das atividades pelo gestor e fiscal do contrato, incluindo verificação de relatórios e auditorias periódicas.

4.17.4. Encerramento ou Renovação

4.17.4.1. Avaliação do Desempenho do Serviço: Análise da qualidade e benefícios obtidos.

4.17.4.2. Tomada de Decisão: Renovação, recontração ou descontinuidade do serviço.

4.17.4.3. Devolução ou Migração de Dados: Plano para migração segura dos dados, se necessário, respeitando requisitos de portabilidade.

4.17.4.4. Encerramento Contratual: Cumprimento de obrigações finais e arquivamento da documentação.

5. REQUISITOS DA CONTRATAÇÃO (Anexo III, Art. 8º, do Decreto 552/24)

5.1. Do consórcio:

5.1.1. Devido a natureza da contratação, ou seja, exclusividade na prestação do serviço, ficaria inviável a contratação de um CONSÓRCIO;

5.1.2. Em um consórcio, a responsabilidade por falhas e problemas pode se tornar difusa, tornando difícil identificar a quem recorrer em caso de questões técnicas ou de serviço.

5.1.3. Com um único fornecedor, é mais fácil estabelecer accountability e garantir que o responsável pela prestação do serviço atenda a todos os requisitos e SLA (Service Level Agreements).

5.1.4. Processos de decisão em consórcios podem ser mais lentos devido à necessidade de consenso entre as partes. A contratação direta com um único fornecedor permite decisões mais ágeis e respostas rápidas a mudanças nas necessidades da organização.

5.1.5. Dessa forma fica vedada a participação de empresas nesse tipo de regime.

5.2. Da Subcontratação

5.2.1. Devido à natureza do objeto ser composta por vários serviços, a subcontratação será parcialmente autorizada mediante formalização feita por parte da CONTRATADA e devidamente autorizada pela equipe técnica da ALETO;

5.2.2. Exigências relacionadas à fase de Habilitação:

5.2.3. Apresentação de no mínimo um atestado emitido por pessoa jurídica de direito público ou privado, comprovando que a proponente fornece/forneceu serviços compatíveis com os objetos da licitação emitidos em papel timbrado, com assinatura, identificação e telefone do emitente;

5.2.4. Não serão aceitos atestados com objeto genérico, ou seja, deverá constar nos respectivos Atestados nomenclatura compatível com os itens licitados. Os atestados deverão ser apresentados em papel timbrado ou com carimbo do CNPJ da pessoa jurídica, contendo a identificação do signatário, ficando reservado à Comissão Permanente de Licitação o direito de solicitar cópias dos contratos e notas fiscais a que se referem tais documentos;

5.2.5. Não serão aceitos documentos que representam a participação da LICITANTE em consórcio e/ou cooperativa para fins de qualificação técnica;

5.2.6. Apresentar declaração da LICITANTE comprovando ciência do Termo de Referência e de que a proposta está de acordo com suas prerrogativas, conforme Declaração de Ciência do Termo de Referência;

5.3. Visita Técnica:

5.3.1. Para este lote, é facultado à proponente realizar vistoria técnica na Sede da CONTRATANTE, localizado na cidade de Palmas - TO, em data agendada para levantamento de informações sobre o local onde estão atualmente instalados os equipamentos de TIC e onde deverá ser instalado o circuito do link LAN-TO-LAN, com intuito de avaliar os serviços e entregas que serão exigidas posteriormente se declarada como vencedora da disputa;

5.3.2. As empresas deverão solicitar o agendamento da vistoria em até 4 (quatro) dias úteis da data da disputa, pelo e-mail cosuti@al.to.leg.br, cujo campo “assunto” da mensagem deverá conter o texto “Vistoria – Edital Serviços de Cloud Computing”. As empresas serão comunicadas por e-mail, dos momentos e local onde devem se apresentar, para a vistoria, e quem as conduzirá. A vistoria será realizada em até 3 (três) dias úteis da data do certame;

5.3.3. Ao final da vistoria, a licitante emitirá Termo em favor da proponente, circunstanciando o atendimento desta exigência. Este Termo deve ser apresentado para a habilitação no certame junto com a documentação exigida. Os custos da vistoria são de responsabilidade da proponente, incluindo seus deslocamentos em veículo próprio ao local vistoriado;

5.3.4. Caso a proponente opte por não realizar vistoria, firmará declaração na qual dispensa a necessidade de vistoria, assumindo todo e qualquer risco por sua decisão e se comprometendo a prestar fielmente o serviço nos termos de sua proposta e do presente Termo de Referência;

5.3.5. O Termo de Vistoria Técnica ou a Declaração de Dispensa de Vistoria deverá ser apresentado juntamente com a documentação relativa à habilitação do certame. Não será permitida a participação de empresas que não atenderam esta exigência, estando automaticamente desclassificadas do certame;

5.3.6. As proponentes se obrigam a não divulgar, publicar ou fazer uso das informações recebidas durante a vistoria. A simples participação na vistoria caracteriza o compromisso irretratável de guarda do sigilo dos dados colhidos.

5.4. Requisitos gerais

5.4.1. Será exigido das licitantes, conforme previsto no artigo 58, da Lei 14.133/2021, garantia da proposta equivalente a 1% (um por cento) do valor estimado para a contratação a que concorre, podendo a licitante optar por uma das seguintes modalidades (artigo 96, parágrafo 1º da Lei 14.133/2021):

5.4.1.1. I - caução em dinheiro ou em títulos da dívida pública emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados por seus valores econômicos, conforme definido pelo Ministério da Economia;

5.4.1.2. II - seguro-garantia;

5.4.1.3. III - fiança bancária emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil.

5.4.2. A futura contratada deverá atender a todas as exigências descritas no Edital, Termo de Referência e documentos que irão compor o certame licitatório;

5.4.3. A contratada deverá preencher todos os requisitos de regularidade jurídica, fiscal, técnica e econômico-financeira, previstos no Decreto Administrativo 552/2024, além de atender ao disposto no inciso XXXIII, do art. 7º, da Constituição Federal;

5.4.4. A duração inicial do contrato deverá ser de até 12 (doze) meses, com a possibilidade de prorrogação contratual conforme os limites legais ou sua rescisão.

5.4.5. A empresa deverá oferecer uma infraestrutura robusta e escalável, com servidores de última geração, redundância de dados e alta disponibilidade.

5.4.6. Deverão ser apresentados protocolos de segurança, como criptografia de dados, firewalls, controles de acesso e procedimentos de resposta a incidentes.

5.4.7. A empresa deverá fornecer suporte técnico 24/7, com equipe qualificada para resolver problemas e garantir a continuidade dos serviços.

5.4.8. A empresa deverá oferecer soluções de backup regular e planos de recuperação de desastres para garantir a integridade e disponibilidade dos dados.

5.4.9. A solução deverá permitir a fácil expansão dos recursos conforme a demanda da Assembleia Legislativa aumentar, sem a necessidade de reestruturações complexas.

5.4.10. Deverão ser definidos SLAs claros que estabeleçam os níveis de serviço esperados, incluindo tempos de resposta e disponibilidade garantida.

5.4.11. A proposta deverá incluir uma estrutura de custos clara e detalhada, evitando surpresas e garantindo que a ALETO possa planejar seu orçamento adequadamente.

5.4.12. A empresa deverá ser capaz de integrar suas soluções com sistemas existentes da Assembleia Legislativa, garantindo uma transição suave e sem interrupções.

5.4.13. A empresa deverá oferecer treinamento para a equipe da ALETO, capacitando-a a utilizar e gerenciar as soluções implementadas.

5.4.14. A empresa deverá ter uma política clara sobre a proteção de dados e a privacidade das informações, assegurando que todos os dados da Assembleia Legislativa sejam tratados de acordo com as normas vigentes.

5.5.Requisitos de Treinamento:

5.5.1. Objetiva a transmissão dos conhecimentos necessários para que a equipe técnica da ALETO suporte o funcionamento da solução;

5.5.2. O Treinamento de administrador avançado deverá fornecer as informações necessárias para o gerenciamento geral da solução, incluindo definições de políticas, configurações de recursos de retenção, permissionamento, controle de dados, acesso e gerenciamento de dispositivos e aplicativos, auditoria e outros;

5.5.3. O treinamento para usuários finais poderá ser remoto ou presencial, com carga horária mínima de 3 horas e deverá abordar as informações necessárias à utilização geral de todos os aplicativos da plataforma, além de itens como: gerência, administração, auditoria e suporte interno da solução.

5.5.4. A CONTRATADA deverá comunicar previamente à turma a data de realização do treinamento, sendo responsabilidade de cada integrante da turma dispor de computador com acesso à internet e webcam;

5.5.5. Ao término do treinamento, deverão ser fornecidos atestados de participação, contendo no mínimo o nome do aluno, assunto, entidade promotora, carga horária, período de realização, ministrante e conteúdo programático.

5.6. Cláusula de Conformidade com a Lei Geral de Proteção de Dados – LGPD

5.6.1. A prestação dos serviços objeto deste Termo de Referência, na modalidade de Infraestrutura como Serviço (IaaS), deverá observar, obrigatoriamente, as disposições da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente no que se refere à proteção, segurança e sigilo de dados eventualmente tratados, armazenados ou processados em virtude da execução contratual.

5.6.2. A empresa contratada deverá:

5.6.2.1. Assegurar a implementação de medidas técnicas e administrativas adequadas à proteção dos dados pessoais armazenados ou trafegados por meio da infraestrutura contratada, protegendo-os contra acessos não autorizados, perda, destruição, alteração, vazamento ou qualquer forma de tratamento inadequado ou ilícito;

5.6.2.2. Garantir a confidencialidade, integridade e disponibilidade dos dados, bem como a rastreabilidade das ações executadas na infraestrutura, por meio de controles de acesso, registros de log e demais ferramentas de auditoria e monitoramento compatíveis com boas práticas de segurança da informação;

5.6.2.3. Preferencialmente, disponibilizar infraestrutura com data centers localizados em território nacional, ou, alternativamente, em países que ofereçam nível de proteção de dados pessoais adequado, conforme definido pela Autoridade Nacional de Proteção de Dados (ANPD);

5.6.2.4. Comprometer-se a notificar imediatamente a ALETO em caso de incidente de segurança que possa comprometer dados pessoais tratados no âmbito do contrato;

5.6.2.5. Não compartilhar dados pessoais com terceiros sem autorização prévia e expressa da ALETO, salvo por força de obrigação legal;

5.6.2.6. Cooperar com a Administração Pública para garantir os direitos do titular de dados, inclusive mediante fornecimento de informações e apoio a eventuais auditorias ou fiscalizações promovidas pela ALETO ou por órgãos de controle.

5.6.2.7. O descumprimento das obrigações acima será considerado infração contratual grave, sujeita às penalidades previstas na legislação aplicável, sem prejuízo das responsabilidades civis, administrativas e penais cabíveis.

5.7. Metas de Nível de Serviço (SLA) – Infraestrutura como Serviço (IaaS)

5.7.1. Para garantir a qualidade da prestação dos serviços contratados, deverão ser observadas, pela contratada, as seguintes metas de desempenho mínimo:

5.7.1.1. Disponibilidade da Infraestrutura (uptime):

5.7.1.1.1. Meta: mínimo de 99,5% de disponibilidade mensal da infraestrutura contratada (servidores, rede, armazenamento).

5.7.1.1.2. A forma de verificação será através de relatórios automáticos e periódicos disponibilizados pela contratada.

5.7.1.1.3. A contratada será submetida a penalidade de abatimento proporcional no valor mensal, conforme tabela de descontos prevista em contrato.

5.7.1.2. Prazo de Atendimento a Incidentes Críticos (ex: falha de servidor ou rede):

5.7.1.2.1. Meta: início do atendimento em até 1 hora após a abertura do chamado.

5.7.1.2.2. Solução completa em até 4 horas, contadas do registro da ocorrência.

5.7.1.3. Prazo de Atendimento a Incidentes de Baixa/Média Complexidade:

5.7.1.3.1. Meta: início do atendimento em até 4 horas úteis após a abertura do chamado.

5.7.1.3.2. Solução completa em até 12 horas úteis, contadas do registro da ocorrência.

5.7.2. Prazo para Provisionamento de Recursos (ex: criação de nova VM, alocação de disco, etc.):

5.7.2.1. Meta: execução da solicitação em até 8 horas úteis após o registro do pedido.

5.7.3. Backup e Recuperação de Dados:

5.7.3.1. Meta: backups automáticos diários e retenção mínima de 7 dias.

5.7.3.2. RTO (Recovery Time Objective): máximo de 4 horas para recuperação de dados sob demanda.

5.7.3.3. RPO (Recovery Point Objective): até 24 horas, ou seja, perda de dados de no máximo um dia.

5.7.4. Canal de Suporte Técnico

5.7.4.1. Meta: disponibilidade de canal de atendimento técnico remoto 24x7, com suporte via e-mail, telefone ou plataforma online.

5.7.5. Relatórios Mensais de Desempenho e Incidentes

5.7.5.1. Meta: envio de relatório mensal contendo:

5.7.5.2. Disponibilidade da infraestrutura;

5.7.5.3. Incidentes registrados e respectivos tempos de resolução;

5.7.5.4. Solicitações atendidas;

5.7.5.5. Ações preventivas e corretivas adotadas.

5.7.6. O quadro com a matriz de Nível de Serviços estará no requisito “Medição e Pagamento” deste Termo de Referência.

5.8. Requisitos do Suporte Técnico:

5.8.1. Os serviços de suporte técnico e de atualização de versão têm por finalidade garantir a sustentação, a plena utilização e atualização da solução durante a vigência do contrato, além de garantir a integridade do conteúdo do contratante mantido pela solução contratada;

5.8.2. Ao suporte técnico compete o esclarecimento de dúvidas relacionadas a instalação, configuração e uso do ambiente em nuvem, ou para correção de problemas, em especial na configuração de parâmetros, falhas, erros, defeitos ou vícios identificados no funcionamento da solução. O serviço poderá ser realizado nas instalações da ALETO ou remotamente;

5.8.3. O suporte técnico deve ser iniciado logo após a assinatura do contrato e deverá ser realizado de forma contínua durante a vigência do contrato, e obrigatoriamente, pelo fabricante da ferramenta ou empresa prestadora de serviços devidamente credenciada.

5.8.4. O serviço de atualização se refere ao fornecimento de novas versões e releases dos produtos da solução lançados no decorrer da vigência do contrato. A contratada deverá comunicar o fato ALETO e aplicar a atualização de forma ativa e transparente ao contratante;

5.8.5. A contratada deverá comunicar formalmente à contratante os meios de acionamento do serviço, como número de telefone e endereço de sítio na Internet

5.9. Certificações e Conformidade:

5.9.1. “Essas certificações ou as comprovações alternativas, serão exigidas apenas na fase contratual do processo.

5.9.2. Compreende-se como indispensável que o provedor de nuvem seja certificado nas normas presentes, objetivando (quando aplicável), dessa forma, resguardar a Administração quanto aos princípios basilares de Segurança da Informação: disponibilidade, integridade, confidencialidade e autenticidade das informações a serem hospedadas em infraestruturas em nuvem.

5.9.3. A empresa deve possuir, no mínimo, as certificações **ISO 27001:2013, ISO 27017:2015 e 27018:2014** ou, alternativamente, demonstrar atender a todos os objetivos e controles das referidas normas, mediante apresentação de políticas, procedimentos, e outros documentos. Qualquer documento deverá ser apresentado em nome do licitante, sendo facultado a ALETO promover diligência destinada a esclarecer ou complementar informações.

5.9.4. **ISSO 27001:2013:** Essa norma exige que as organizações estabeleçam, implementem, mantenham e melhorem continuamente um SGSI, que inclua políticas e procedimentos para gerenciar a segurança da informação. Ela enfatiza a importância da avaliação de riscos, que envolve identificar, analisar e avaliar os riscos à segurança da informação. Com base nessa avaliação, as organizações devem implementar controles adequados para mitigar os riscos identificados.

5.9.5. **ISO 27017:2015:** Norma que fornece diretrizes para os controles de segurança de informação aplicáveis à prestação e utilização de serviços em nuvem, fornecendo o seguinte: diretrizes adicionais para implementação de controles relevantes especificados na ISO/IEC 27002; controles adicionais com diretrizes de implementação relacionadas especificamente a serviços em nuvem.

5.9.6. **ISO 27018:2014:** Essa norma estabelece objetivos de controle e diretrizes comumente aceitos para implementação de medidas para proteger as informações de identificação Pessoal (PII) consoante com os princípios de privacidade descritos na ISO/IEC 29100, para o ambiente de computação em nuvem.

5.9.7. A nova Lei de Licitações (Lei nº 14.133/2021) permite que a Administração Pública estabeleça requisitos de habilitação o qual os licitantes devem cumprir para participar do processo licitatório.

5.9.8. Esses requisitos podem incluir a apresentação de certificados de qualidade ou conformidade, desde que sejam relevantes para o objeto da contratação.

“artigo 42 – a prova de qualidade do produto apresentado pelos proponentes como similar ao das

marcas eventualmente indicadas no edital será admitida por qualquer um dos seguintes meios:

I - Comprovação de que o produto está de acordo com as normas técnicas determinadas pelos órgãos oficiais competentes, pela Associação Brasileira de Normas Técnicas (ABNT) ou por outra entidade credenciada pelo Inmetro;

III - certificação, certificado, laudo laboratorial ou documento similar que possibilite a aferição da qualidade e da conformidade do produto ou do processo de fabricação, inclusive sob o aspecto ambiental, emitido por instituição oficial competente ou por entidade credenciada.

§ 1º O edital poderá exigir, como condição de aceitabilidade da proposta, certificação de qualidade do produto por instituição credenciada pelo Conselho Nacional de Metrologia, Normalização e Qualidade Industrial (Conmetro)”

5.9.9. Considerando a existência de uma gama de riscos de segurança, inerente ao armazenamento de informações em ambientes externos a ALETO, toma-se necessário que o provedor de nuvem assuma rígidos padrões de segurança. Conforme legislação em vigor e termo de compromisso assinado, a contratada responderá caso ocorra divulgação ou utilização de informações sigilosas, as quais tenha obtido acesso em virtude do contrato. Em hipótese alguma poderá ser divulgada os dados da ALETO, que tenha acesso por motivo contratual.

5.9.10. A contratada deverá adotar todas as medidas necessárias para assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações a serem tratadas na nuvem. E, igualmente, deverá implementar medidas para garantir a proteção dos dados, antecipando ameaças à privacidade, à segurança e à integridade, prevenindo acesso não autorizado às informações.

5.9.11. Por fim, exigir certificações ISO é perfeitamente justificado, uma vez que o seu principal objetivo é ajudar as organizações a protegerem suas informações de forma sistemática e eficaz, garantindo a confidencialidade, integridade e disponibilidade dos dados. Essas normas fornecem uma estrutura para a implementação de controles de segurança e para a gestão de riscos relacionados à segurança da informação.

6. PROVA DE CONCEITO – POC

6.1. Após a fase de habilitação da documentação será realizada a Prova de Conceito (POC), convocada pelo pregoeiro, com objetivo de averiguar se a licitante arrematante cumpre com os requisitos presentes neste Termo de Referência;

6.2. Será realizada uma diligência, composta por membros indicados pela CONTRATANTE, para avaliação da Prova de Conceito, bem como posterior elaboração de parecer técnico, levando em consideração as exigências aqui contidas;

6.3. O início da Prova de Conceito se dará em até 30 (trinta) dias corridos, contados da data da convocação;

6.4. O fim da Prova de Conceito se dará em até 3 (três) dias úteis, contados do seu início. Encerrado o prazo de 3 (três) dias úteis os resultados serão avaliados por equipe técnica da CONTRATANTE.

6.5. Encerrado o prazo de 3 (três) dias úteis para a execução da prova de conceito, os resultados alcançados serão avaliados por equipe técnica da CONTRATANTE em até 5 dias úteis, contados a partir do dia seguinte ao término da prova de conceito;

6.6. O agendamento com a unidade técnica da CONTRATANTE para a realização da prova de conceito deverá ser feito em dias úteis das 10h às 17h;

6.7. A licitante que não agendar a realização da prova de conceito ou não a executar nos prazos estipulados terá sua proposta desclassificada, conforme definido no edital;

6.8. Na diligência será verificado a aderência as exigências deste termo de referência, obedecendo o roteiro abaixo:

Roteiro da Prova de Conceito		
Item	Atividade	Descrição / Requisitos mandatórios a serem apresentados
1	Vistoria física no ambiente da prestação do serviço	▪ Vistoria física no ambiente para prestação do serviço de Colocation para equipamentos de TIC, do licitante arrematante para verificação da aderência do ambiente aos requisitos exigidos no item “ESPECIFICAÇÕES DO AMBIENTE DE DATA CENTER”, tais como, mas não se limitando a: ✓ Instalações elétricas; ✓ Sistema de Climatização; ✓ Características do Cabeamento Estruturado LAN/SAN; ✓ Sistema de Controle de Acesso e Monitoramento; ✓ Verificação da existência do ambiente e ferramentas de NOC, para a apoio a operação 24x7;
2	Validar link requisitos do link LAN-TO-LAN	▪ A arrematante deve, em um prazo de até 15 (quinze) dias, instalar no ambiente da CONTRATANTE um link LAN-TO-LAN com velocidade de 1Gbps, interligando este ambiente ao ambiente de seu Data Center, onde deverão ser demonstrando o atendimento às seguintes exigências: ✓ Latência igual ou inferior à 5ms; ✓ Largura de banda igual a 1Gbps; ✓ Perda de pacotes inferior a 2%; ▪ A aferição dos requisitos acima se dará em um prazo de 24 horas após a instalação do link, onde serão iniciados os testes com o link em funcionamento por no mínimo 4h (quatro horas) ininterruptas;

7. MODELO DE EXECUÇÃO DO OBJETO (Anexo III, Art.13, do Decreto 552/24)

Os serviços deverão ser prestados/entregues conforme discriminado abaixo:

7.1. Informações Gerais:

7.1.1. A empresa CONTRATADA assume o compromisso de iniciar o processo de implantação no prazo de 07 (sete) dias, após a reunião inicial, e a conclusão da implantação de

todos os serviços delineados no Termo de Referência em um prazo não excedente a 30 (trinta) dias consecutivos, podendo ser prorrogados por igual período, desde que justificado.

7.1.2. A mencionada implantação abrange todos os elementos, características, funcionalidades e especificações mencionadas nos segmentos precedentes.

7.1.3. Na eventualidade de não conformidade com qualquer um dos requisitos solicitados, será considerado um desvio aos termos contratados.

7.1.4. Ao longo do período de implantação, a empresa CONTRATADA compromete-se a manter o CONTRATANTE informado acerca do progresso, apresentando relatórios periódicos e permanecendo disponível para elucidar eventuais dúvidas ou inquietações que possam surgir.

7.1.5. A operacionalização, transporte e a realização dos serviços no(s) local(is) estabelecido(s) pelo CONTRATANTE deverão ser executados pela CONTRATADA, de maneira a observar sua aceitação.

7.1.6. A operacionalização, instalação, transporte e a realização dos serviços no(s) local(is) estabelecido(s) pelo CONTRATANTE deverão ser executados pela CONTRATADA, de maneira a observar sua aceitação.

7.1.7. Caberá à empresa proceder à instalação do sistema e à implementação dos serviços necessários, dentro das normas gerais pertinentes.

7.1.8. Todos os custos para execução dos serviços, como análises, contratação de terceiros, deslocamentos, estadas, alimentação, material de consumo, transportes, instalação e o que necessitar para a conclusão dos serviços, são de responsabilidade da contratada;

7.2. Da Migração do Ambiente

7.2.1. A CONTRATADA deverá conduzir a Migração do Ambiente da ALETO, que está atualmente hospedado em seu Datacenter, para as suas dependências no novo Datacenter;

7.2.2. A reunião inicial entre a equipe da ALETO e da CONTRATADA, para apresentação do PREPOSTO desta última e início das atividades de absorção de conhecimentos, não poderá ultrapassar os primeiros 10 dias úteis após a assinatura do contrato;

7.2.3. Após o período de absorção de conhecimentos, a CONTRATADA deverá apresentar estratégia de migração para o ambiente, para análise e aprovação do plano pela equipe técnica da ALETO;

7.2.4. A Migração do Ambiente deverá ocorrer preferencialmente em finais de semana ou após o horário de expediente normal da ALETO visando minimizar eventual impacto sobre a rotina dos usuários finais de sistemas informatizados;

7.3. Da implantação dos serviços:

7.3.1. Os recursos para uso nos serviços de nuvem serão fornecidos como um pool computacional de processadores virtuais, gigabytes de memória, espaço em disco (mecânico e SSD), licença para Windows Server e espaço para backups, que serão utilizados de modo a atender aos requisitos de disponibilidade e desempenho das aplicações;

7.3.2. Servidores virtuais Linux podem utilizar sistemas operacionais que não necessitem de licenciamento (Ubuntu ou CentOS) e, neste caso, não impactarão nas de licenças;

7.3.3. A migração do ambiente de Datacenter atual da ALETO para o disponibilizado pela CONTRATADA fará uso desse pool de recursos, cuja alocação poderá ser aumentada, até o limite máximo previsto no contrato, ou reduzida, de acordo com as necessidades computacionais da CONTRATANTE;

7.3.4. Os recursos do pool poderão ser alocados ou removidos de máquinas virtuais existentes, conforme definição da equipe técnica da ALETO, desde que abaixo do teto previsto em contrato;

7.3.5. As alterações nas configurações ou comportamento das máquinas virtuais, como alocação e remoção de recursos, clonagem, ligação, desligamento ou reinicialização, deverão ser permitidos à equipe técnica da ALETO através de interface de ferramenta de orquestração;

7.3.6. O serviço de backup é a cópia e salvaguarda dos dados do ambiente da CONTRATANTE, incluindo as imagens de máquinas virtuais, compartilhamentos de arquivos na rede, bancos de dados de aplicações e diretórios internos nas máquinas virtuais, conforme definido pela equipe técnica da ALETO.

7.3.7. A CONTRATADA deverá fornecer informações suficientes para que a equipe técnica da ALETO possa avaliar as políticas efetivamente implementadas ou, alternativamente, acesso às ferramentas para validação de implementação de tais políticas, para a tomada de decisão e adequação do uso de recursos.

7.3.8. A Migração total dos dados, sistemas e serviços da ALETO deverá ser finalizada em até 120 (cento e vinte) dias a partir da assinatura do contrato e será supervisionada pela equipe técnica da ALETO em conjunto com Gerente de Projeto definido pela CONTRATANTE;

7.3.9. Durante a Migração do Ambiente propriamente dita, a CONTRATADA deverá realizar as seguintes atividades:

7.3.10. Cópia de todos os dados do ambiente de TIC e de todos os subsistemas de armazenamento de dados da ALETO para o Datacenter da CONTRATADA;

7.3.11. A verificação da consistência dos dados copiados com vistas a assegurar a preservação de sua integridade;

7.3.12. A remoção definitiva dos dados nos subsistemas de origem de forma a permitir que eles sejam desativados sem por em risco a confidencialidade dos dados.

7.3.13. A implantação abrange todos os elementos, características, funcionalidades e especificações mencionadas nos segmentos precedentes.

7.3.14. Na eventualidade de não conformidade com qualquer um dos requisitos solicitados, será considerado um desvio aos termos contratados.

7.3.15. Ao longo do período de implantação, a empresa CONTRATADA compromete-se a manter o CONTRATANTE informado acerca do progresso, apresentando relatórios periódicos e permanecendo disponível para elucidar eventuais dúvidas ou inquietações que possam surgir.

7.3.16. A operacionalização, transporte e a realização dos serviços nos locais estabelecidos) pelo CONTRATANTE deverão ser executados pela CONTRATADO, de maneira a observar sua aceitação.

8. MODELO DE GESTÃO DO CONTRATO (Anexo III, Art. 10, Inciso I, do Decreto 552/24)

8.1. Das disposições Gerais

8.1.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas do Decreto Administrativo 552 de 2024 Anexo X, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

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

8.1.3. As comunicações entre a ALETO e a CONTRATADA devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

8.1.4. A ALETO poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

8.1.5. Após a assinatura do contrato para o serviço de migração do ambiente atual para a nuvem, a ALETO poderá convocar o representante da 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.

8.2.Preposto

8.2.1. Antes do início da prestação dos serviços, a CONTRATADA deverá designar formalmente o preposto da empresa, com, no mínimo, nome completo, CPF e canais de contato (e-mail e telefones corporativos). Este procedimento será realizado por meio de um documento contendo o logotipo da empresa e a assinatura digital do representante legal da CONTRATADA, no qual serão claramente estabelecidos os poderes e deveres do preposto em relação à execução do objeto contratado.

8.2.2. O Preposto da Contratada deverá estar acessível em horário comercial (9h às 18h) pelos canais indicados, não cabendo a presença no ambiente da ALETO.

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

8.3. Reunião Inicial

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

8.3.2. A reunião ocorrerá em até 10 dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da CONTRATANTE.

8.3.3. A pauta desta reunião observará, pelo menos:

8.3.3.1. Presença do representante legal da CONTRATADA, que apresentará o seu preposto;

8.3.3.2. Entrega, por parte da CONTRATADA, do Termo de Compromisso e dos Termos de

Ciência;

8.3.3.3. esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

8.3.3.4. O preposto será o funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor principal junto à CONTRATANTE, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

8.4.Da fiscalização

8.4.1. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos.

8.4.2. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração;

8.4.3. O fiscal técnico do contrato anotar no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados.

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

8.4.5. O fiscal técnico do contrato informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso;

8.4.6. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato;

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

8.4.8. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência.

8.4.9. Caso ocorram descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência;

8.4.10. O gestor do contrato coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de fornecimento, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração.

8.4.11. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico e administrativo quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações.

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

8.4.13. O fiscal administrativo do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou prorrogação contratual.

8.4.14. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração.

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

8.4.16. O contratado deverá manter preposto aceito pela Administração no local da entrega para representá-lo na execução do contrato.

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

9. DA FORMALIZAÇÃO E RECEBIMENTO DOS SERVIÇOS (Capítulo VIII, Seção II, Art. 62, Parágrafo 1º, Inciso II, do Decreto 552/24)

O recebimento dos serviços obedecerá a seguinte demanda

a) **provisoriamente:** O Fiscal Técnico do contrato receberá o relatório da prestação dos serviços fornecido pela contratada e irá fazer a verificação se todo o serviço descrito nesse relatório foi devidamente prestado de acordo com o contrato.

b) **definitivamente**: Uma vez feita esta verificação e a sua confirmação pelo Fiscal Técnico do contrato dos serviços prestado, o gestor do contrato irá autorizar a contratada a emitir documento fiscal para prosseguir com o pagamento da mesma.

§2º Os prazos e os métodos específicos para a realização dos recebimentos provisório e definitivo serão definidos no contrato.

De acordo com o Art. 63 do decreto 552/24, as atividades de gestão e fiscalização devem observar o princípio da segregação das funções e as seguintes diretrizes:

I - o recebimento **provisório** será realizado pelo fiscal, por meio de relatório detalhado contendo o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, o qual deverá ser encaminhado ao gestor do contrato ou à comissão designada pela autoridade competente para recebimento definitivo, juntamente com documentos comprobatórios, quando for o caso.

II - o recebimento **definitivo** pelo gestor do contrato ou comissão designada será realizado por meio das seguintes atividades:

a) análise dos relatórios e de toda a documentação apresentada pela fiscalização técnica e administrativa e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicação das cláusulas contratuais pertinentes e solicitação à contratada, por escrito, das respectivas correções;

b) emissão de termo detalhado para efeito de recebimento definitivo do objeto, com base nos relatórios e documentação apresentados.

10. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO (Anexo III, Art. 16 do Decreto 552/24)

10.1. Da forma de medição

10.1.1. Uma vez por mês a contratada deverá informar através de relatório ou outro documento equivalente os serviços que foram executados, no documento deverá constar detalhadamente cada item utilizado a ser pago, tais itens não devem de maneira alguma estar fora do escopo desse projeto, o fiscal técnico do contrato será o responsável por validar os serviços e quantitativos descritos no relatório, uma vez essas informações validadas pelo fiscal, o gestor do contrato irá autorizar a contratada emitir a nota fiscal para prosseguir os tramites para o pagamento.

10.1.2. Não serão considerados serviços passíveis de pagamento, a simples alocação de espaço nos servidores da CONTRATADA.

10.2. Do prazo para a realização do pagamento

10.2.1. O pagamento será realizado em até 30 (vinte) dias, contados a partir do atesto da Administração na fatura apresentada, cujo prazo é de até 05 (cinco) dias úteis.

10.2.2. O pagamento será realizado somente depois de relatório emitido pelo fiscal do contrato confirmado a real prestação dos serviços cobrados.

10.3. Da forma de pagamento

10.3.1. O pagamento devido a CONTRATADA será efetuado por meio de Ordem Bancária, mediante a apresentação da nota fiscal, atestada e visada pelo Departamento de Tecnologia da Informação, responsável pela Gestão, fiscalização e acompanhamento do recebimento do material, no prazo estipulado neste Termo de Referência.

10.3.2. Na Nota Fiscal/Fatura deverá conter obrigatoriamente a informação da instituição bancária, o número da agência e o número da conta bancária, cujo titular seja a CONTRATADA.

10.3.3. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período.

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

10.3.5. 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:

10.3.5.1. O prazo de validade;

10.3.5.2. A data da emissão;

10.3.5.3. Os dados do contrato e do órgão CONTRATANTE;

10.3.5.4. O período respectivo de execução do contrato;

10.3.5.5. O valor a pagar; e

10.3.5.6. Eventual destaque do valor de retenções tributárias cabíveis.

10.3.6. 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;

10.3.7. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais.

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

10.3.9. Constatando-se, junto ao SICAF, a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do CONTRATANTE.

10.3.10. Não havendo regularização ou sendo a defesa considerada improcedente, o CONTRATANTE deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

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

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

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

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

10.4. Matriz de Nível de Serviço (SLA) – IaaS

Indicador de Desempenho	Meta esperada	Peso (%)	Penalidade por Descumprimento
-------------------------	---------------	----------	-------------------------------

Disponibilidade da Infraestrutura	≥ 99,5% por mês	40 %	Multa de 2% sobre o valor mensal por cada 0,1% abaixo da meta; abaixo de 98%, suspensão contratual.
Tempo de Resposta a Incidentes Críticos	Atendimento em até 1h	15 %	Redução de 1% no valor mensal por cada hora de atraso.
Tempo de Solução de Incidentes Críticos	Solução em até 4h	10 %	Redução de 2% no valor mensal por ocorrência fora do prazo.
Tempo de Solução de Incidentes Menores	Solução em até 12h úteis	10 %	Redução de 1% no valor mensal por cada ocorrência fora do prazo.
Provisionamento de Recursos	Em até 8h úteis	10 %	Redução de 1% no valor mensal por ocorrência fora do prazo.
Backup e Recuperação de Dados (RTO ≤ 4h)	RTO ≤ 4h / RPO ≤ 24h	10 %	Redução de 3% no valor mensal por falha ou atraso.
Relatórios Mensais de Desempenho	Envio até o 5º dia útil	5 %	Redução de 0,5% por dia de atraso.

10.4.1. Critério de Avaliação Global do SLA

10.4.1.1. Acima de 95% da pontuação total - Desempenho excelente, sem penalidades;

10.4.1.2. Entre 85% e 94,9% - Desempenho aceitável, com advertência formal;

10.4.1.3. Abaixo de 85% - Desempenho insatisfatório, sujeitando-se à aplicação de sanções contratuais e análise de possível rescisão.

10.5. Penalidades por Inexecução Contratual

Sem prejuízo das sanções administrativas previstas na Lei nº 14.133/2021, a contratada estará sujeita às seguintes penalidades pecuniárias, sempre que ocorrer inexecução total ou parcial das obrigações contratuais, inclusive o descumprimento de metas de SLA:

10.5.1. Descumprimento de Metas de SLA

10.5.1.1. Aplicação de descontos no valor mensal devido, conforme matriz de SLA definida neste Termo de Referência.

10.5.1.2. Em caso de reincidência por 2 (dois) meses consecutivos ou 3 (três) intercalados dentro de um período de 6 (seis) meses, a Administração poderá aplicar, cumulativamente:

10.5.1.2.1. Advertência;

10.5.1.2.2. Multa de 2% (dois por cento) sobre o valor global do contrato.

10.5.2. Atraso no Início da Prestação do Serviço

10.5.2.1. Multa de 0,5% (meio por cento) por dia de atraso, limitada a 10% (dez por cento) do valor global do contrato.

10.5.3. Interrupção Não Justificada do Serviço

10.5.3.1. Multa de 1% (um por cento) por hora de interrupção injustificada, limitada a 20% (vinte por cento) do valor mensal da fatura.

10.5.4. Falha na Execução de Backups ou Recuperação de Dados

10.5.4.1. Multa de 3% (três por cento) por ocorrência, sobre o valor mensal, quando houver falha comprovada e não justificada na realização dos backups ou no atendimento ao RTO/RPO estabelecidos.

10.5.5. Não Entrega de Relatórios de Desempenho

10.5.5.1. Multa de 0,5% (meio por cento) por dia de atraso, limitada a 5% (cinco por cento) do valor mensal da fatura.

10.6. Disposição Final

10.6.1. As penalidades pecuniárias aqui previstas poderão ser aplicadas cumulativamente com sanções administrativas, observando-se o contraditório e a ampla defesa, conforme art. 156 da Lei nº 14.133/2021. Os valores das multas poderão ser descontados de eventuais pagamentos devidos ou cobrados judicialmente.

11. FORMA DE CONTRATAÇÃO E CRITÉRIO DE SELEÇÃO DO FORNECEDOR (Anexo III, Art. 7º, do Decreto 552/24)

11.1. O fornecedor deverá ser selecionado por meio da realização de procedimento **LICITATÓRIO** na modalidade **PREGÃO**, preferencialmente sob a forma **ELETRÔNICA**, com adoção do critério de julgamento pelo **MENOR PREÇO GLOBAL** e modo de lances **“ABERTO”**, a adjudicação será por **LOTE**.

11.2. Tendo em vista se tratar de contratação de serviços comuns disponível no mercado, conforme já manifestado no ETP, a contratação em tela não se enquadra em técnica e preços e conforme é amplamente praticada na administração pública em pregões similares.

11.3. Por fim, o uso do Sistema de Registro de Preços justifica-se por ser a forma preferencial de aquisição, conforme o **Art. 36, Inciso IV, do Capítulo V do Decreto 552/24**. Ademais, trata de procedimento visando contratações futuras, cuja definição da demanda não é possível ser previamente quantificada com precisão. Finalmente, a utilização do SRP propiciará a redução de custos, sem a realização de licitações seguidas para o mesmo objeto, atendendo-se, portanto, aos princípios da economicidade, celeridade e eficiência.

11.4. Ante o exposto e fundamentado na possibilidade de registro de preços propostas pela Lei no 14.133/2021, que dentre as novidades possibilita vantajosidade e economicidade dos órgãos públicos na prorrogação de validade de ARPs por período de até 24 (vinte e quatro) meses. E que a ALETO vem evoluindo exponencialmente em seu processo de transformação digital, trabalhando cada vez mais na inovação e maior proximidade com seu usuário final (Servidores, Deputados e cidadãos tocantinenses), torna-se vantajoso o registro de quantitativo, sendo pertinente relatar que as próprias operadoras desse tipo de serviço recomendam tal forma de evolução, haja vista os custos de um processo licitatório e o tempo depreendido para o cumprimento de todo o fluxo administrativo.

11.5. Os documentos referentes a habilitação e comprovação econômico financeira do licitante será tratado no Edital.

12. ESTIMATIVA DO VALOR DA CONTRATAÇÃO (Decreto 552/24, Capítulo II, Art. 9º e seus parágrafos)

O custo estimado total **mensal** da contratação é de **R\$ 225.170,00** obtidos a partir de pesquisas de preços juntadas aos autos do processo licitatório, para todo o objeto, conforme valores unitários e totais apresentados na planilha de preço médio.

LOTE 01				
ITEM	DESCRIÇÃO	QTD	V. UNIT.	V. TOTAL
1	SERVIÇOS DE VCPU	200	R\$ 83,33	R\$ 16.666,67
2	SERVIÇOS DE MEMORIA RAM	400	R\$ 41,00	R\$ 16.400,00
3	SERVIÇOS DE ARMAZENAMENTO EM BLOCO NVME (GB)	12.000	R\$ 2,07	R\$ 24.800,00
4	SERVIÇOS DE ARMAZENAMENTO EM BLOCO HDD (GB)	70.000	R\$ 0,90	R\$ 63.000,00

5	SERVIÇOS DE LINK LAN-TO-LAN (MB)	1.000	R\$ 9,00	R\$ 9.000,00
6	SERVIÇOS DE LINK DE INTERNET (MB)	1.000	R\$ 12,49	R\$ 12.490,00
7	SERVIÇOS DE LICENÇAS WINDOWS SERVER	80	R\$ 41,00	R\$ 3.280,00
08	SERVIÇOS GERENCIADOS DE FIREWALL	2	R\$ 9.333,33	R\$ 18.666,67
09	SERVIÇOS GERENCIADOS DE ANTIVÍRUS	50	R\$ 116,67	R\$ 5.833,33
10	SERVIÇOS GERENCIADOS DE BACKUP	50	R\$ 163,33	R\$ 8.166,67
11	SERVIÇOS DE NOC (PCT 10 ATIVOS)	50	R\$ 393,33	R\$ 19.666,67
12	SERVIÇOS TÉCNICOS ESPECIALIZADOS (HORAS)	80	R\$ 340,00	R\$ 27.200,00
VALOR ESTIMADO DO PROJETO/ MÊS				R\$ 225.170,00

13. ADEQUAÇÃO ORÇAMENTÁRIA

13.1.A aquisição será custeada com recursos próprios da Assembleia Legislativa do Estado do Tocantins, referente ao exercício de 2024.

13.2.Os Elementos da despesa serão indicados pela Diretoria de Execução Orçamentária Financeira e estarão discriminadas nos autos do processo.

14. DAS OBRIGAÇÕES DA CONTRATADA (Anexo III, Art. 12 do Decreto 552/24)

14.1. Assegurar-se através da vistoria, que o local de instalação dos equipamentos necessários à prestação dos serviços, possui as condições técnicas e ambientais necessárias ao funcionamento dos equipamentos necessários aos serviços;

14.2.Especificar e requerer da CONTRANTE as condições técnicas e ambientais para a instalação das soluções em no máximo 48 (quarenta e oito) horas úteis do recebimento da solicitação de serviço para implantação da solução;

14.3.Implantar todos os softwares e hardwares necessários à prestação dos serviços de monitoração, gerência e administração remota da segurança, conforme as especificações técnicas constantes deste Termo de Referência;

14.4.Todas as soluções de hardware e software, ambientes de gerenciamento e monitoramento devem ser fornecidos em regime de locação;

14.5.Iniciar a prestação dos serviços dentro dos prazos estabelecidos neste Termo de Referência;

14.6.As implantações das soluções serão realizadas pela CONTRATADA e todas as atividades envolvidas serão acompanhadas e coordenadas por analistas e técnicos da CONTRANTE;

14.7.A CONTRATADA na implantação da solução, quando realizada no ambiente de produção, deverá ter a disponibilidade para executar determinadas atividades após o expediente (horários noturnos ou em finais de semana e feriados);

14.8.A CONTRATADA deverá fornecer às senhas de configuração dos equipamentos, se existirem, a CONTRANTE, onde designará três pessoas para terem acesso a(s) senha(s), que devem ser fornecidas de forma segura. A CONTRANTE deverá seguir os procedimentos documentais acordados entre as partes, caso venha a fazer uso deste acesso, e se responsabilizará pelas consequências que por ventura possam advir deste acesso;

14.9.A CONTRATADA será responsável por efetuar as atividades de integração da solução de monitoramento remoto com o ambiente operacional da CONTRANTE, sem prejuízo aos serviços desta;

14.10.Registrar os tempos de atendimento dos chamados de suporte técnico ou chamados de serviços;

14.11.Garantir e manter total e absoluto sigilo sobre as informações manuseadas, as quais devem ser utilizadas apenas para a condução das atividades autorizadas, não podendo ter quaisquer outros usos, sob pena de rescisão contratual e medidas cíveis e penais cabíveis, assumindo inteira responsabilidade pelo uso indevido ou ilegal de informações privilegiadas da

CONTRANTE, praticado por seus empregados, conforme Acordo de Responsabilidade para Fornecedores, a ser assinado pela CONTRATADA no ato da assinatura do contrato;

14.12. Não subcontratar total ou parcialmente os serviços objeto do certame, com outra empresa, sem prévia anuência por escrito da contratante, sob pena de incorrer na rescisão do contrato;

14.13. A CONTRATADA deverá disponibilizar, durante todo o período do contrato, todos os equipamentos e softwares necessários à execução dos serviços.

15. OBRIGAÇÕES DA CONTRATANTE

15.1. Providenciar as condições técnicas e ambientais necessárias à implantação e funcionamento dos serviços;

15.2. Providenciar as autorizações de acesso aos técnicos da CONTRATADA, desde que devidamente agendado e os técnicos identificados, aos locais de instalação das soluções para as implantações e nos casos de manutenções;

15.3. Informar aos técnicos da CONTRATADA as necessidades de configuração dos equipamentos se forem disponibilizados, e serviços. Estas informações serão repassadas para a CONTRATADA através da abertura de chamados de suporte técnico. Quando necessário, podem ser anexados aos chamados arquivos com as necessidades de configurações;

15.4. Cumprir pontualmente todos os seus compromissos financeiros para com a CONTRATADA;

15.5. Proporcionar todas as facilidades para que a CONTRATADA possa executar os serviços de que trata este Termo de Referência, dentro das normas e condições estabelecidas em contrato;

15.6. Comunicar à CONTRATADA todas as possíveis irregularidades detectadas na execução dos serviços contratados, para a pronta correção das irregularidades apontadas;

15.7. Fiscalizar diretamente a execução dos serviços de que trata o objeto deste Termo de Referência, atestando a sua prestação se, e somente se, os serviços executados atenderem plenamente às especificações constantes deste Termo de Referência;

15.8. Rejeitar, no todo ou em parte, a solução entregue pela CONTRATADA fora das especificações deste Termo de Referência;

15.9. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da CONTRATADA pelos danos causados a CONTRANTE ou a terceiros, resultantes de ação ou omissão culposa ou dolosa de quaisquer de seus empregados ou prepostos;

15.10. Responsabilizar-se pelo zelo e proteção de todos os equipamentos da CONTRADADA que forem instalados localmente para propiciar a execução dos serviços. Em caso de dano, avaria ou extravio dos equipamentos, ocasionado por mal-uso ou ausência de segurança do ambiente, a CONTRATANTE deverá ressarcir a CONTRATADA dos prejuízos, conforme valores de mercado das soluções utilizadas;

16. DAS INFRAÇÕES E SANÇÕES ADMINISTRATIVAS (Capítulo VIII, Seção IV, Art. 66, do Decreto 552/24)

O contratado será responsabilizado administrativamente pelas seguintes infrações:

I - dar causa à inexecução parcial do contrato;

II - dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

III - dar causa à inexecução total do contrato;

IV - deixar de entregar a documentação exigida para o certame;

V - não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

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

VII - ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

VIII - apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;

IX - fraudar a licitação ou praticar ato fraudulento na execução do contrato;

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

XI - praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

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

De acordo com o Art. 156 da Lei 14.133/21, serão aplicadas ao responsável pelas infrações administrativas previstas nesta Lei as seguintes sanções:

I - advertência;

II - multa;

III - impedimento de licitar e contratar;

IV - declaração de inidoneidade para licitar ou contratar.

§ 1º Na aplicação das sanções serão considerados:

I - a natureza e a gravidade da infração cometida;

II - as peculiaridades do caso concreto;

III - as circunstâncias agravantes ou atenuantes;

IV - os danos que dela provierem para a Administração Pública;

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

AMÉLIO CAYRES

Presidente

ALEX SANTOS NERES

Diretor de Área de Tecnologia da Informação - DTI

JOÃO GARIBALDI NETO

Diretor DINFRE

MÁRCIO BEZERRA DE OLIVEIRA

Coordenador COSUTI

Palmas do Tocantins, 28 de Abril de 2025.

ANEXO II MINUTA DA ATA DE REGISTRO DE PREÇOS

ATA DE REGISTRO DE PREÇOS N.º/2025

A Assembleia Legislativa do Estado do Tocantins, com sede na Praça dos Girassóis, Palácio João D'Abreu, Centro, na cidade de Palmas – TO, inscrita no CNPJ/MF sob o nº 25.053.125/0001-00, neste ato representada pelo seu Presidente, Deputado Amélio Cayres, conforme ato de posse publicado no Diária da Assembleia, considerando o julgamento da licitação para Registro de Preços na modalidade de pregão, na forma eletrônica nº/2025, processo administrativo nº 0217/2025, em sessão realizada em ____/____/2025, RESOLVE registrar os preços da(s) empresa(s) indicada(s) e qualificada(s) nesta ATA, de acordo com a classificação por ela(s) alcançada(s) e na(s) quantidade(s) cotada(s), atendendo as condições previstas no Edital de licitação, sujeitando-se as partes às normas constantes na Lei nº 14.133, de 1º de abril de 2021, e em conformidade com as disposições a seguir:

1. DO OBJETO

1.1. A presente Ata tem por objeto o registro de preços para a eventual ou futura contratação de XXXXXXXXXXXXXXX, especificado(s) no Termo de Referência, anexo I do edital de Licitação nº/2025, que é parte integrante desta Ata, assim como as propostas cujos preços tenham sido registrados, independentemente de transcrição.

2. DOS PREÇOS, ESPECIFICAÇÕES E QUANTITATIVOS

2.1. O preço registrado, as especificações do objeto, as quantidades máximas de cada item, fornecedor(es) e as demais condições ofertadas na(s) proposta(s) são as que seguem:

Fornecedor:						
CNPJ:			Inscrição Estadual :			
Endereço:		Telefone:	E-mail:	Representante Legal:		
ITEM	UND	QTD	DESCRIÇÃO	Vlr Unit.	Vlr mensal	Valor anual
Valor total						

2.2. A listagem do cadastro de reserva referente ao presente registro de preços, se houver, consta como anexo a esta Ata.

3. ÓRGÃO GERENCIADOR

3.1. O gerenciador que fará o controle de adesões, será a Diretoria de Licitação.

4. DA ADESÃO À ATA DE REGISTRO DE PREÇOS

4.1. Durante a vigência da ata, os órgãos e as entidades da Administração Pública estadual, distrital e municipal que não participaram do procedimento licitatório poderão aderir à ata de registro de preços na condição de não participantes, desde que autorizado, observados os seguintes requisitos:

4.2.1. apresentação de justificativa da vantagem da adesão, inclusive em situações de provável desabastecimento ou descontinuidade de serviço público;

- 4.2.2. demonstração de que os valores registrados estão compatíveis com os valores praticados pelo mercado na forma do art. 23 da Lei nº 14.133, de 2021; e
- 4.2.3. consulta e aceitação prévias do órgão ou da entidade gerenciadora e do fornecedor.
- 4.3. A autorização do órgão ou entidade gerenciadora apenas será realizada após a aceitação da adesão pelo fornecedor.
- 4.3.1. O órgão ou entidade gerenciadora poderá rejeitar adesões caso elas possam acarretar prejuízo à execução de seus próprios contratos ou à sua capacidade de gerenciamento.
- 4.4. Após a autorização do órgão ou da entidade gerenciadora, o órgão ou entidade não participante deverá efetivar a aquisição ou a contratação solicitada em até 90 (noventa) dias, observado o prazo de vigência da ata.
- 4.5. O prazo de que trata o subitem anterior, relativo à efetivação da contratação, poderá ser prorrogado excepcionalmente, mediante solicitação do órgão ou da entidade não participante aceita pelo órgão ou pela entidade gerenciadora, desde que respeitado o limite temporal de vigência da ata de registro de preços.
- 4.6. Dos limites para as adesões:
- 4.6.1 As aquisições ou contratações adicionais não poderão exceder, por órgão ou entidade, a 50% (cinquenta por cento) dos quantitativos dos itens do instrumento convocatório registrados na ata de registro de preços para o gerenciador e para os participantes.
- 4.6.2 O quantitativo decorrente das adesões não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços, independentemente do número de órgãos ou entidades não participantes que aderirem à ata de registro de preços.
- 4.7. Vedação a acréscimo de quantitativos:
- 4.7.1. É vedado efetuar acréscimos nos quantitativos fixados na ata de registro de preços.

5. VALIDADE, FORMALIZAÇÃO DA ATA DE REGISTRO DE PREÇOS E CADASTRO RESERVA

- 5.1. A validade da Ata de Registro de Preços será de 01 (um) ano, contado a partir do primeiro dia útil subsequente à data de divulgação em sítio oficial, podendo ser prorrogada por igual período com restabelecimento total dos seus quantitativos iniciais, mediante a anuência do fornecedor, desde que comprovado o preço vantajoso.
- 5.2. O contrato decorrente da ata de registro de preços terá sua vigência estabelecida no próprio instrumento contratual e observará no momento da contratação e a cada exercício financeiro a disponibilidade de créditos orçamentários, bem como a previsão no plano plurianual, quando ultrapassar 1 (um) exercício financeiro.
- 5.2.1. Na formalização do contrato ou do instrumento substituto deverá haver a indicação da disponibilidade dos créditos orçamentários respectivos.
- 5.3. A contratação com os fornecedores registrados na ata será formalizada pelo órgão ou pela entidade interessada por intermédio de instrumento contratual, emissão de nota de empenho de despesa, autorização de compra ou outro instrumento hábil, conforme o art. 95 da Lei nº 14.133, de 2021.
- 5.4. O instrumento contratual de que trata o item 5.2 deverá ser assinado no prazo de validade da ata de registro de preços.
- 5.5. Os contratos decorrentes do registro de preços poderão ser alterados, observado o art. 124 da Lei nº 14.133, de 2021.
- 5.6. Após a homologação da licitação, deverão ser observadas as seguintes condições para formalização da ata de registro de preços:
- 5.6.1. Serão registrados na ata os preços e os quantitativos do adjudicatário, devendo o licitante se obrigar aos limites dela;

- 5.6.2. Será incluído na ata, na forma de anexo, o registro dos licitantes ou dos fornecedores que:
- 5.6.2.1. Aceitarem cotar os bens, as obras ou os serviços com preços iguais aos do adjudicatário, observada a classificação da licitação; e
- 5.6.2.2. Mantiverem sua proposta original.
- 5.6.3. Será respeitada, nas contratações, a ordem de classificação dos licitantes ou dos fornecedores registrados na ata.
- 5.7. O registro a que se refere o item 5.6.2 tem por objetivo a formação de cadastro de reserva para o caso de impossibilidade de atendimento pelo signatário da ata.
- 5.8. Para fins da ordem de classificação, os licitantes ou fornecedores que aceitarem reduzir suas propostas para o preço do adjudicatário antecederão aqueles que mantiverem sua proposta original.
- 5.9. A habilitação dos licitantes que comporão o cadastro de reserva a que se refere o item “5.6.2” somente será efetuada quando houver necessidade de contratação dos licitantes remanescentes, nas seguintes hipóteses:
- 5.9.1. Quando o licitante vencedor não assinar a ata de registro de preços, no prazo e nas condições estabelecidos no edital ou no aviso de contratação direta; e
- 5.9.2. Quando houver o cancelamento do registro do licitante ou do registro de preços nas hipóteses previstas no item 9.
- 5.10. O preço registrado com indicação dos licitantes e fornecedores será divulgado em sítio oficial e ficará disponibilizado durante a vigência da ata de registro de preços.
- 5.11. Após a homologação da licitação ou da contratação direta, o licitante mais bem classificado, será convocado para assinar a ata de registro de preços, no prazo e nas condições estabelecidos no edital de licitação, sob pena de decair o direito, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021.
- 5.10.1. O prazo de convocação poderá ser prorrogado 1 (uma) vez, por igual período, mediante solicitação do licitante ou fornecedor convocado, desde que apresentada dentro do prazo, devidamente justificada, e que a justificativa seja aceita pela Administração.
- 5.11. A ata de registro de preços poderá assinada por meio de assinatura digital.
- 5.12. Quando o convocado não assinar a ata de registro de preços no prazo e nas condições estabelecidos no edital, fica facultado à Administração convocar os licitantes remanescentes do cadastro de reserva, na ordem de classificação, para fazê-lo em igual prazo e nas condições propostas pelo primeiro classificado, e observado o disposto no item 5.9 e subitens.
- 5.13. Na hipótese de nenhum dos licitantes que trata o item 5.6.2.1, aceitar a contratação nos termos do item anterior, a Administração, observados o valor estimado e sua eventual atualização nos termos do edital ou do aviso de contratação direta, poderá:
- 5.13.1. Convocar para negociação os demais licitantes ou fornecedores remanescentes cujos preços foram registrados sem redução, observada a ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário; ou
- 5.13.2. Adjudicar e firmar o contrato nas condições ofertadas pelos licitantes ou fornecedores remanescentes, atendida a ordem classificatória, quando frustrada a negociação de melhor condição.
- 5.14. A existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas, mas não obrigará a Administração a contratar, facultada a realização de licitação específica para a aquisição pretendida, desde que devidamente justificada.

6. ALTERAÇÃO OU ATUALIZAÇÃO DOS PREÇOS REGISTRADOS

6.1. Os preços registrados poderão ser alterados ou atualizados em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos bens, das obras ou dos serviços registrados, nas seguintes situações:

6.1.1. Em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução da ata tal como pactuada, nos termos da alínea “d” do inciso II do caput do art. 124 da Lei nº 14.133, de 2021;

6.1.2. Em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou a superveniência de disposições legais, com comprovada repercussão sobre os preços registrados;

6.1.3. Na hipótese de previsão no edital de cláusula de reajustamento ou repactuação sobre os preços registrados, nos termos da Lei nº 14.133, de 2021.

6.1.3.1. No caso do reajustamento, deverá ser respeitada a contagem da anualidade e o índice previstos para a contratação;

6.1.3.2. No caso da repactuação, poderá ser a pedido do interessado, conforme critérios definidos para a contratação.

7. NEGOCIAÇÃO DE PREÇOS REGISTRADOS

7.1. Na hipótese de o preço registrado tornar-se superior ao preço praticado no mercado por motivo superveniente, o órgão ou entidade gerenciadora convocará o fornecedor para negociar a redução do preço registrado.

7.1.1. Caso não aceite reduzir seu preço aos valores praticados pelo mercado, o fornecedor será liberado do compromisso assumido quanto ao item registrado, sem aplicação de penalidades administrativas.

7.1.2. Na hipótese prevista no item anterior, o gerenciador convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam reduzir seus preços aos valores de mercado e não convocará os licitantes ou fornecedores que tiveram seu registro cancelado.

7.1.3. Se não obtiver êxito nas negociações, o órgão ou entidade gerenciadora procederá ao cancelamento da ata de registro de preços, adotando as medidas cabíveis para obtenção de contratação mais vantajosa.

7.1.4. Na hipótese de redução do preço registrado, o gerenciador comunicará aos órgãos e às entidades que tiverem firmado contratos decorrentes da ata de registro de preços para que avaliem a conveniência e a oportunidade de diligenciar negociação com vistas à alteração contratual, observado o disposto no art. 124 da Lei nº 14.133, de 2021.

7.2. Na hipótese de o preço de mercado tornar-se superior ao preço registrado e o fornecedor não poder cumprir as obrigações estabelecidas na ata, será facultado ao fornecedor requerer ao gerenciador a alteração do preço registrado, mediante comprovação de fato superveniente que supostamente o impossibilite de cumprir o compromisso.

7.2.1. Neste caso, o fornecedor encaminhará, juntamente com o pedido de alteração, a documentação comprobatória ou a planilha de custos que demonstre a inviabilidade do preço registrado em relação às condições inicialmente pactuadas.

7.2.2. Não hipótese de não comprovação da existência de fato superveniente que inviabilize o preço registrado, o pedido será indeferido pelo órgão ou entidade gerenciadora e o fornecedor deverá cumprir as obrigações estabelecidas na ata, sob pena de cancelamento do seu registro, nos termos do item 9.1, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021, e na legislação aplicável.

7.2.3. Na hipótese de cancelamento do registro do fornecedor, nos termos do item anterior, o gerenciador convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam manter seus preços registrados, observado o disposto no item 5.7.

7.2.4. Se não obtiver êxito nas negociações, o órgão ou entidade gerenciadora procederá ao cancelamento da ata de registro de preços, nos termos do item 9.4, e adotará as medidas cabíveis para a obtenção da contratação mais vantajosa.

7.2.5. Na hipótese de comprovação da majoração do preço de mercado que inviabilize o preço registrado, conforme previsto no item 7.2 e no item 7.2.1, o órgão ou entidade gerenciadora atualizará o preço registrado, de acordo com a realidade dos valores praticados pelo mercado.

7.2.6. O órgão ou entidade gerenciadora comunicará aos órgãos e às entidades que tiverem firmado contratos decorrentes da ata de registro de preços sobre a efetiva alteração do preço registrado, para que avaliem a necessidade de alteração contratual, observado o disposto no art. 124 da Lei nº 14.133, de 2021.

8. REMANEJAMENTO DAS QUANTIDADES REGISTRADAS NA ATA DE REGISTRO DE PREÇOS

8.1. As quantidades previstas para os itens com preços registrados nas atas de registro de preços, não serão remanejadas pelo órgão ou entidade gerenciadora entre os órgãos ou as entidades não participantes do registro de preços.

9. CANCELAMENTO DO REGISTRO DO LICITANTE VENCEDOR E DOS PREÇOS REGISTRADOS

9.1. O registro do fornecedor será cancelado pelo gerenciador, quando o fornecedor:

9.1.1. Descumprir as condições da ata de registro de preços, sem motivo justificado;

9.1.2. Não retirar a nota de empenho, ou instrumento equivalente, no prazo estabelecido pela Administração sem justificativa razoável;

9.1.3. Não aceitar manter seu preço registrado, nas hipóteses previstas na legislação; ou

9.1.4. Sofrer sanção prevista nos incisos III ou IV do caput do art. 156 da Lei nº 14.133, de 2021.

9.1.4.1. Na hipótese de aplicação de sanção prevista nos incisos III ou IV do caput do art. 156 da Lei nº 14.133, de 2021, caso a penalidade aplicada ao fornecedor não ultrapasse o prazo de vigência da ata de registro de preços, poderá o órgão ou a entidade gerenciadora poderá, mediante decisão fundamentada, decidir pela manutenção do registro de preços, vedadas contratações derivadas da ata enquanto perdurarem os efeitos da sanção.

9.2. O cancelamento de registros nas hipóteses previstas no item 9.1 será formalizado por despacho do órgão ou da entidade gerenciadora, garantidos os princípios do contraditório e da ampla defesa.

9.3. Na hipótese de cancelamento do registro do fornecedor, o órgão ou a entidade gerenciadora poderá convocar os licitantes que compõem o cadastro de reserva, observada a ordem de classificação.

9.4. O cancelamento dos preços registrados poderá ser realizado pelo gerenciador, em determinada ata de registro de preços, total ou parcialmente, nas seguintes hipóteses, desde que devidamente comprovadas e justificadas:

9.4.1. Por razão de interesse público;

9.4.2. A pedido do fornecedor, decorrente de caso fortuito ou força maior; ou

9.4.3. Se não houver êxito nas negociações, nas hipóteses em que o preço de mercado tornar-se superior ou inferior ao preço registrado.

10. DAS PENALIDADES

10.1. O descumprimento da Ata de Registro de Preços ensejará aplicação das penalidades estabelecidas no edital.

10.1.1. As sanções também se aplicam aos integrantes do cadastro de reserva no registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente após terem assinado a ata.

10.2. É da competência do gerenciador a aplicação das penalidades decorrentes do descumprimento do pactuado nesta ata de registro de preço, exceto nas hipóteses em que o descumprimento disser respeito às contratações dos órgãos ou entidade participante, caso no qual caberá ao respectivo órgão participante a aplicação da penalidade.

10.3. O órgão ou entidade participante deverá comunicar ao órgão gerenciador qualquer das ocorrências previstas no item 9.1, dada a necessidade de instauração de procedimento para cancelamento do registro do fornecedor.

11. CONDIÇÕES GERAIS

11.1. As condições gerais de execução do objeto, tais como os prazos para entrega e recebimento, as obrigações da Administração e do fornecedor registrado, penalidades e demais condições do ajuste, encontram-se definidos no Termo de Referência, Anexo ao Edital.

11.2. No caso de adjudicação por preço global de grupo de itens, só será admitida a contratação de parte de itens do grupo se houver prévia pesquisa de mercado e demonstração de sua vantagem para o órgão ou a entidade.

Para firmeza e validade do pactuado, a presente Ata foi lavrada em 02 (duas) vias de igual teor, que, depois de lida e achada em ordem, vai assinada pelas partes.

Palmas, TO, aos ____ de _____ de 2025

Assinaturas

**ANEXO III
MINUTA DO CONTRATO**

**TERMO DE CONTRATO Nº ____/2025,
CELEBRADO ENTRE A ASSEMBLEIA
LEGISLATIVA DO TOCANTINS - TO E A
EMPRESA _____ VISANDO A
_____ (RESUMO DO OBJETO).**

CONTRATANTE: ASSEMBLEIA LEGISLATIVA DO TOCANTINS, instituição de direito público, inscrita no Ministério da Fazenda sob o nº _____, com sede na XXXXXXXX, em Palmas, Estado do Tocantins, neste ato representado pela sr. XXXXXXXX Presidente da Aleto, XXXXXX CPF _____, brasileiro, casado, residente em XXXXXXXX.

CONTRATADA: _____, pessoa jurídica de direito privado, com sede na _____, inscrita no Ministério da Fazenda sob o nº _____, por seu Representante Legal, _____, CPF _____ têm justos e certos o presente Contrato, mediante as Cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA - FUNDAMENTO LEGAL

1.1. Tendo em vista o que consta no **Processo nº 0217/2025** e em observância às disposições da Lei nº 14.133, de 1º de abril de 2021, e demais legislação aplicável, resolvem celebrar o presente Termo de Contrato, decorrente do **Pregão Eletrônico nº ____/2025**, mediante as cláusulas e condições a seguir enunciadas.

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

2.1. Constitui objeto do presente a contratação de pessoa jurídica especializada em prestação de serviços de **xxxxxxxxxxxxxxxxxxxx**, conforme quantidades e condições estabelecidas no Edital e seus anexos.

2.2. Discriminação do objeto da contratação:

ITEM	DESCRIÇÃO	QTDE	UNID	VALOR UNIT. (R\$)	VALOR TOTAL MENSAL (R\$)	VALOR TOTAL ANUAL (R\$)
VALOR TOTAL						

2.3. Vinculam esta contratação, independentemente de transcrição:

- 2.3.1. O Termo de Referência;
- 2.3.2. O Edital da Licitação;
- 2.3.3. A Proposta do contratado;
- 2.3.4. Eventuais anexos dos documentos supracitados.

CLÁUSULA TERCEIRA – VIGÊNCIA E PRORROGAÇÃO

3.1. O prazo inicial de vigência da contratação é de 12 (doze) meses contados da assinatura do Termo contratual, na forma do artigo 105 da Lei nº 14.133, de 2021.

3.1.1. Por se tratar de serviços contínuos, essenciais para o desenvolvimento das atividades da Assembleia Legislativa, o contrato poderá ser prorrogado sucessivamente, até o limite decenal, caso as condições e preços permaneçam vantajosos para a administração, conforme previsto no art. 107 da Lei nº 14.133/2021.

CLÁUSULA QUARTA– SUBCONTRATAÇÃO

- 4.1. Não será admitida a subcontratação parcial do objeto contratual, sem a devida anuência da contratante.
- 4.2. Não será permitida a subcontratação da parcela principal do objeto.

CLÁUSULA QUINTA – MODELO DE EXECUÇÃO E GESTÃO CONTRATUAL (art. 92, IV, VII e XVIII)

5.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas do Decreto Administrativo 552 de 2024 Anexo X, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

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

5.3. As comunicações entre a Aleto e a CONTRATADA devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

5.4. A Aleto poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

5.5. Após a assinatura do contrato para o serviço de migração do ambiente atual para a nuvem, a Aleto poderá convocar o representante da 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.

Informações Gerais:

5.5.1. A empresa CONTRATADA assume o compromisso de iniciar o processo de implantação no prazo de 07 (sete) dias, após a reunião inicial, e a conclusão da implantação de todos os serviços delineados no Termo de Referência em um prazo não excedente a 30 (trinta) dias consecutivos, podendo ser prorrogados por igual período, desde que justificado.

5.5.2. A mencionada implantação abrange todos os elementos, características, funcionalidades e especificações mencionadas nos segmentos precedentes.

5.5.3. Na eventualidade de não conformidade com qualquer um dos requisitos solicitados, será considerado um desvio aos termos contratados.

5.5.4. Ao longo do período de implantação, a empresa CONTRATADA compromete-se a manter o CONTRATANTE informado acerca do progresso, apresentando relatórios periódicos e permanecendo disponível para elucidar eventuais dúvidas ou inquietações que possam surgir.

5.5.5. A operacionalização, transporte e a realização dos serviços no(s) local(is) estabelecido(s) pelo CONTRATANTE deverão ser executados pela CONTRATADA, de maneira a observar sua aceitação.

5.5.6. Caberá à empresa proceder à instalação do sistema e à implementação dos serviços necessários, dentro das normas gerais pertinentes.

5.5.7. Todos os custos para execução dos serviços, como análises, contratação de terceiros, deslocamentos, estadas, alimentação, material de consumo, transportes, instalação e o que necessitar para a conclusão dos serviços, são de responsabilidade da contratada;

5.6. Migração do Ambiente

5.6.1. A CONTRATADA deverá conduzir a Migração do Ambiente da Aleto, que está atualmente hospedado em seu Datacenter, para as suas dependências no novo Datacenter;

5.6.2. A reunião inicial entre a equipe da Aleto e da CONTRATADA, para apresentação do PREPOSTO desta última e início das atividades de absorção de conhecimentos, não poderá ultrapassar os primeiros 10 dias úteis após a assinatura do contrato;

5.6.3. Após o período de absorção de conhecimentos, a CONTRATADA deverá apresentar estratégia de migração para o ambiente, para análise e aprovação do plano pela equipe técnica da Aleto;

5.6.4. A Migração do Ambiente deverá ocorrer preferencialmente em finais de semana ou após o horário de expediente normal da Aleto visando minimizar eventual impacto sobre a rotina dos usuários finais de sistemas informatizados;

5.7. Implantação dos serviços:

5.7.1. Os recursos para uso nos serviços de nuvem serão fornecidos como um pool computacional de processadores virtuais, gigabytes de memória, espaço em disco (mecânico e SSD), licença para Windows Server e espaço para backups, que serão utilizados de modo a atender aos requisitos de disponibilidade e desempenho das aplicações;

5.7.2. Servidores virtuais Linux podem utilizar sistemas operacionais que não necessitem de licenciamento (Ubuntu ou CentOS) e, neste caso, não impactarão nas de licenças;

5.7.3. A migração do ambiente de Datacenter atual da Aleto para o disponibilizado pela CONTRATADA fará uso desse pool de recursos, cuja alocação poderá ser aumentada, até o limite máximo previsto no contrato, ou reduzida, de acordo com as necessidades computacionais da CONTRATANTE;

5.7.4. Os recursos do pool poderão ser alocados ou removidos de máquinas virtuais existentes, conforme definição da equipe técnica da Aleto, desde que abaixo do teto previsto em contrato;

5.7.5. As alterações nas configurações ou comportamento das máquinas virtuais, como alocação e remoção de recursos, clonagem, ligação, desligamento ou reinicialização, deverão ser permitidos à equipe técnica da Aleto através de interface de ferramenta de orquestração;

5.7.6. O serviço de backup é a cópia e salvaguarda dos dados do ambiente da CONTRATANTE, incluindo as imagens de máquinas virtuais, compartilhamentos de arquivos na rede, bancos de dados de aplicações e diretórios internos nas máquinas virtuais, conforme definido pela equipe técnica da Aleto.

5.7.7. A CONTRATADA deverá fornecer informações suficientes para que a equipe técnica da Aleto possa avaliar as políticas efetivamente implementadas ou, alternativamente, acesso às ferramentas para validação de implementação de tais políticas, para a tomada de decisão e adequação do uso de recursos.

5.7.8. A Migração total dos dados, sistemas e serviços da Aleto deverá ser finalizada em até 120 (cento e vinte) dias a partir da assinatura do contrato e será supervisionada pela equipe técnica da Aleto em conjunto com Gerente de Projeto definido pela CONTRATANTE;

5.7.9. Durante a Migração do Ambiente propriamente dita, a CONTRATADA deverá realizar as seguintes atividades:

5.7.10. Cópia de todos os dados do ambiente de TIC e de todos os subsistemas de armazenamento de dados da Aleto para o Datacenter da CONTRATADA;

5.7.11. A verificação da consistência dos dados copiados com vistas a assegurar a preservação de sua integridade;

5.7.12. A remoção definitiva dos dados nos subsistemas de origem de forma a permitir que eles sejam desativados sem por em risco a confidencialidade dos dados.

5.7.13. A implantação abrange todos os elementos, características, funcionalidades e especificações mencionadas nos segmentos precedentes.

5.7.14. Na eventualidade de não conformidade com qualquer um dos requisitos solicitados, será considerado um desvio aos termos contratados.

5.7.15. Ao longo do período de implantação, a empresa CONTRATADA compromete-se a manter o CONTRATANTE informado acerca do progresso, apresentando relatórios periódicos e permanecendo disponível para elucidar eventuais dúvidas ou inquietações que possam surgir.

5.7.16. A operacionalização, transporte e a realização dos serviços nos locais estabelecidos) pelo CONTRATANTE deverão ser executados pela CONTRATADO, de maneira a observar sua aceitação.

5.8. Preposto:

5.8.1. Antes do início da prestação dos serviços, a CONTRATADA deverá designar formalmente o preposto da empresa, com, no mínimo, nome completo, CPF e canais de contato (e-mail e telefones corporativos). Este procedimento será realizado por meio de um documento contendo o logotipo da empresa e a assinatura digital do representante legal da CONTRATADA, no qual serão claramente estabelecidos os poderes e deveres do preposto em relação à execução do objeto contratado.

5.8.1.1. O Preposto da Contratada deverá estar acessível em horário comercial (9h às 18h) pelos canais indicados, não cabendo a presença no ambiente da ALETO.

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

5.8.1.3. O preposto será o funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor principal junto à CONTRATANTE, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

5.9. Fiscalização:

5.9.1. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos.

5.9.2. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração;

5.9.3. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados.

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

5.9.5. O fiscal técnico do contrato informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso;

5.9.6. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato;

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

5.9.8. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassem a sua competência.

5.9.9. Caso ocorram descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência;

5.9.10. O gestor do contrato coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de fornecimento, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração.

5.9.11. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico e administrativo quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações.

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

5.9.13. O fiscal administrativo do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou prorrogação contratual.

5.9.14. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração.

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

5.9.16. O contratado deverá manter preposto aceito pela Administração no local da entrega para representá-lo na execução do contrato.

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

5.10. Execução do contrato:

5.10.1. A Aleto poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

5.10.2. Caberá à empresa fornecer aos funcionários todos os equipamentos de proteção individual de uso obrigatório pelos empregados exigidos pela legislação.

5.10.3. A CONTRATADA estará obrigada a atender diariamente a todas as ordens de serviço expedidas durante a vigência do contrato.

5.10.4. A equipe técnica da CONTRATADA deverá contar com profissionais especializados e devidamente habilitados para desenvolverem as diversas atividades necessárias à execução dos serviços.

5.10.5. A qualquer tempo, a CONTRATANTE poderá solicitar, por motivo justificado, a substituição de qualquer membro da equipe técnica da CONTRATADA.

5.10.6. Os materiais a serem empregados devem ser de ótima qualidade, sendo que a CONTRATANTE poderá recusar aplicação de substitutos que julgar não convenientes à manutenção de desempenho ou vida útil dos sistemas.

5.10.7. Todos os custos deverão estar incluídos nos preços unitários constantes da proposta da CONTRATADA.

5.10.8. Caberá à CONTRATADA o fornecimento de uniformes e equipamentos de proteção individual à sua equipe técnica.

5.10.9. A operacionalização, instalação, transporte e a realização dos serviços no(s) local(is) estabelecido(s) pelo CONTRATANTE deverão ser executados pela CONTRATADA, de maneira a observar sua aceitação.

5.10.10. Caberá à empresa proceder à instalação do sistema e à implementação dos serviços necessários, dentro das normas gerais pertinentes.

5.10.11. Todos os custos para execução dos serviços, como análises, contratação de terceiros, deslocamentos, estadas, alimentação, material de consumo, transportes, instalação e o que necessitar para a conclusão dos serviços, são de responsabilidade da contratada;

5.10.12. A prestação dos serviços será de responsabilidade da empresa contratada, devendo ser incluídos todos os eventuais custos indiretos, tais como entrega, deslocamento/transporte, carga e descarga dos bens e alimentação dos prepostos.

5.11. Recebimento dos serviços:

5.11.1. Os serviços serão recebidos:

a) Provisoriamente: O Fiscal Técnico do contrato receberá o relatório da prestação dos serviços fornecido pela contratada e irá fazer a verificação se todo o serviço descrito nesse relatório foi devidamente prestado de acordo com o contrato.

b) Definitivamente: Uma vez feita esta verificação e a sua confirmação pelo Fiscal Técnico do contrato dos serviços prestado, o gestor do contrato irá autorizar a contratada a emitir documento fiscal para prosseguir com o pagamento da mesma.

5.11.2 De acordo com o Art. 63 do decreto 552/24, as atividades de gestão e fiscalização devem observar o princípio da segregação das funções e as seguintes diretrizes:

I - O recebimento provisório será realizado pelo fiscal, por meio de relatório detalhado contendo o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, o qual deverá ser encaminhado ao gestor do contrato ou à comissão designada pela autoridade competente para recebimento definitivo, juntamente com documentos comprobatórios, quando for o caso.

II - O recebimento definitivo pelo gestor do contrato ou comissão designada será realizado por meio das seguintes atividades:

a) análise dos relatórios e de toda a documentação apresentada pela fiscalização técnica e administrativa e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicação das cláusulas contratuais pertinentes e solicitação à contratada, por escrito, das respectivas correções;

b) emissão de termo detalhado para efeito de recebimento definitivo do objeto, com base nos relatórios e documentação apresentados.

5.12. Critérios de avaliação dos níveis de serviços:

5.12.1 Matriz de Nível de Serviço (SLA) – IaaS

Indicador de Desempenho	Meta esperada	Peso (%)	Penalidade por Descumprimento
Disponibilidade da Infraestrutura	$\geq 99,5\%$ por mês	40 %	Multa de 2% sobre o valor mensal por cada 0,1% abaixo da meta; abaixo de 98%, suspensão contratual.
Tempo de Resposta a Incidentes Críticos	Atendimento em até 1h	15 %	Redução de 1% no valor mensal por cada hora de atraso.
Tempo de Solução de Incidentes Críticos	Solução em até 4h	10 %	Redução de 2% no valor mensal por ocorrência fora do prazo.
Tempo de Solução de Incidentes Menores	Solução em até 12h úteis	10 %	Redução de 1% no valor mensal por cada ocorrência fora do prazo.
Provisionamento de Recursos	Em até 8h úteis	10 %	Redução de 1% no valor mensal por ocorrência fora do prazo.
Backup e Recuperação de Dados ($RTO \leq 4h$)	$RTO \leq 4h$ / $RPO \leq 24h$	10 %	Redução de 3% no valor mensal por falha ou atraso.
Relatórios Mensais de Desempenho	Envio até o 5º dia útil	5 %	Redução de 0,5% por dia de atraso.

5.12.2. Critério de Avaliação Global do SLA:

- Acima de 95% da pontuação total - Desempenho excelente, sem penalidades;
- Entre 85% e 94,9% - Desempenho aceitável, com advertência formal;
- Abaixo de 85% - Desempenho insatisfatório, sujeitando-se à aplicação de sanções contratuais e análise de possível rescisão.

5.12.3. Penalidades por Inexecução Contratual:

5.12.3.1 Sem prejuízo das sanções administrativas previstas na Lei nº 14.133/2021, a contratada estará sujeita às seguintes penalidades pecuniárias, sempre que ocorrer inexecução total ou parcial das obrigações contratuais, inclusive o descumprimento de metas de SLA:

5.12.3.2. Descumprimento de Metas de SLA

5.12.3.2.1. Aplicação de descontos no valor mensal devido, conforme matriz de SLA.

5.12.3.2.2. Em caso de reincidência por 2 (dois) meses consecutivos ou 3 (três) intercalados dentro de um período de 6 (seis) meses, a Administração poderá aplicar, cumulativamente:

- Advertência;
- Multa de 2% (dois por cento) sobre o valor global do contrato.

5.12.3.2.3. Atraso no Início da Prestação do Serviço

- Multa de 0,5% (meio por cento) por dia de atraso, limitada a 10% (dez por cento) do valor global do contrato.

5.12.3.2.4. Interrupção Não Justificada do Serviço

a) Multa de 1% (um por cento) por hora de interrupção injustificada, limitada a 20% (vinte por cento) do valor mensal da fatura.

5.12.3.2.5. Falha na Execução de Backups ou Recuperação de Dados

a) Multa de 3% (três por cento) por ocorrência, sobre o valor mensal, quando houver falha comprovada e não justificada na realização dos backups ou no atendimento ao RTO/RPO estabelecidos.

5.12.3.2.6. Não Entrega de Relatórios de Desempenho

a) Multa de 0,5% (meio por cento) por dia de atraso, limitada a 5% (cinco por cento) do valor mensal da fatura.

5.12.4. As penalidades pecuniárias aqui previstas poderão ser aplicadas cumulativamente com sanções administrativas, observando-se o contraditório e a ampla defesa, conforme art. 156 da Lei nº 14.133/2021. Os valores das multas poderão ser descontados de eventuais pagamentos devidos ou cobrados judicialmente.

CLÁUSULA SEXTA - PREÇO (art. 92, V)

6.1. O valor total da contratação é de R\$...... (.....)

6.1.1. Serão pagos mensalmente os valores correspondentes aos quantitativos de serviços entregues para uso da Aleto naquele período, observando-se os valores unitários mensais para cada item e quantitativos máximos constantes da tabela do item 2.2 da Cláusula segunda deste instrumento.

6.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, salários, benefícios, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, seguros, e outros necessários ao cumprimento integral do objeto da contratação.

CLÁUSULA SÉTIMA – PAGAMENTO (art. 92, V e VI)

7.1. Forma de medição dos serviços:

7.1.1. Uma vez por mês a contratada deverá informar através de relatório ou outro documento equivalente os serviços que foram executados, no documento deverá constar detalhadamente cada item utilizado a ser pago, tais itens não devem de maneira alguma estar fora do escopo desse projeto, o fiscal técnico do contrato será o responsável por validar os serviços e quantitativos descritos no relatório, uma vez essas informações validadas pelo fiscal, o gestor do contrato irá autorizar a contratada emitir a nota fiscal para prosseguir os trâmites para o pagamento.

7.1.2. Não serão considerados serviços passíveis de pagamento, a simples alocação de espaço nos servidores da CONTRATADA.

7.2. Prazo para a realização do pagamento:

7.2.1. O pagamento será realizado em até 30 (trinta) dias, contados a partir do atesto da Administração na fatura apresentada, cujo prazo é de até 05 (cinco) dias úteis.

7.2.2. O pagamento será realizado somente depois de relatório emitido pelo fiscal do contrato confirmado a real prestação dos serviços cobrados.

7.3. Forma de pagamento

7.3.1. O pagamento devido a CONTRATADA será efetuado por meio de Ordem Bancária, mediante a apresentação da nota fiscal, atestada e visada pelo Departamento de Tecnologia da Informação, responsável pela Gestão, fiscalização e acompanhamento do recebimento do material, no prazo estipulado neste Termo de Referência.

7.3.2. Na Nota Fiscal/Fatura deverá conter obrigatoriamente a informação da instituição bancária, o número da agência e o número da conta bancária, cujo titular seja a CONTRATADA.

- 7.3.3. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período.
- 7.3.4. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.
- 7.3.5. 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:
- 7.3.5.1. O prazo de validade;
 - 7.3.5.2. A data da emissão;
 - 7.3.5.3. Os dados do contrato e do órgão CONTRATANTE;
 - 7.3.5.4. O período respectivo de execução do contrato;
 - 7.3.5.5. O valor a pagar; e
 - 7.3.5.6. Eventual destaque do valor de retenções tributárias cabíveis.
- 7.3.6. 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;
- 7.3.7. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais.
- 7.3.8. A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.
- 7.3.9. Constatando-se, junto ao SICAF, a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do CONTRATANTE.
- 7.3.10. Não havendo regularização ou sendo a defesa considerada improcedente, o CONTRATANTE deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.
- 7.3.11. Persistindo a irregularidade, o CONTRATANTE deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.
- 7.3.12. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação junto ao SICAF.
- 7.3.13. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.
- 7.3.14. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

CLÁUSULA OITAVA - DO REAJUSTAMENTO DE PREÇOS (art. 92, V)

8.1 Após o interregno de um ano, mediante solicitação da Contratada, os preços iniciais dos serviços poderão ser reajustados.

8.1.1. Para fins de apuração do interregno de 01 ano, a data de referência para início de contagem é o da elaboração do orçamento (mapa de preços) da licitação.

8.2.1. O reajuste solicitado pela Contratada deve se referir à atualização dos valores decorrentes às percas pela inflação, sendo que o respectivo reajuste será apurado mediante a aplicação do Índice Nacional de Preços ao Consumidor Amplo - IPCA, acumulado para o respectivo período.

8.2.2. No caso de atraso ou não divulgação do índice de reajustamento, a Contratante pagará à Contratada a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo; fica a Contratada obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.

8.3. Nos reajustes subsequentes ao primeiro, o interregno de um ano será computado do último reajuste correspondente à mesma parcela objeto de nova solicitação. Entende-se como último reajuste, a data em que foram iniciados seus efeitos financeiros, independentemente daquela em que celebrado ou apostilado.

8.4. Os novos valores contratuais decorrentes dos reajustes terão suas vigências iniciadas observando-se o seguinte:

- a) a partir da ocorrência do fato gerador que deu causa ao reajuste;
- b) em data futura, desde que acordada entre as partes, sem prejuízo da contagem de periodicidade para concessão dos próximos reajustes futuros.

8.5. Os efeitos financeiros do reajuste ficarão restritos exclusivamente aos itens que o motivaram, e apenas em relação à diferença porventura existente.

8.6. A concessão do simples reajuste poderá ser realizado por Apostilamento.

CLÁUSULA NONA – OBRIGAÇÕES DA CONTRATANTE (art. 92, X, XI e XIV)

9.1. São obrigações da contratante:

- a) Providenciar as condições técnicas e ambientais necessárias à implantação e funcionamento dos serviços;
- b) Providenciar as autorizações de acesso aos técnicos da CONTRATADA, desde que devidamente agendado e os técnicos identificados, aos locais de instalação das soluções para as implantações e nos casos de manutenções;
- c) Informar aos técnicos da CONTRATADA as necessidades de configuração dos equipamentos se forem disponibilizados, e serviços. Estas informações serão repassadas para a CONTRATADA através da abertura de chamados de suporte técnico. Quando necessário, podem ser anexados aos chamados arquivos com as necessidades de configurações;
- d) Cumprir pontualmente todos os seus compromissos financeiros para com a CONTRATADA;
- e) Proporcionar todas as facilidades para que a CONTRATADA possa executar os serviços, dentro das normas e condições estabelecidas em contrato;
- f) Comunicar à CONTRATADA todas as possíveis irregularidades detectadas na execução dos serviços contratados, para a pronta correção das irregularidades apontadas;
- g) Fiscalizar diretamente a execução dos serviços, atestando a sua prestação se, e somente se, os serviços executados atenderem plenamente às especificações constantes do Termo de Referência;
- h) Rejeitar, no todo ou em parte, a solução entregue pela CONTRATADA fora das especificações do Termo de Referência;
- i) A fiscalização por parte da Contratante não exclui nem reduz a responsabilidade da CONTRATADA pelos danos causados a CONTRANTE ou a terceiros, resultantes de ação ou omissão culposa ou dolosa de quaisquer de seus empregados ou prepostos;

j) Responsabilizar-se pelo zelo e proteção de todos os equipamentos da CONTRADADA que forem instalados localmente para propiciar a execução dos serviços. Em caso de dano, avaria ou extravio dos equipamentos, ocasionado por mal-uso ou ausência de segurança do ambiente, a CONTRATANTE deverá ressarcir a CONTRATADA dos prejuízos, conforme valores de mercado das soluções utilizadas.

CLÁUSULA DÉCIMA – OBRIGAÇÕES DO CONTRATADO (art. 92, XIV, XVI e XVII)

10.1. São obrigações da Contratada:

- a) Assegurar-se através da vistoria, que o local de instalação dos equipamentos necessários à prestação dos serviços, possui as condições técnicas e ambientais necessárias ao funcionamento dos equipamentos necessários aos serviços;
- b) Especificar e requerer da CONTRANTE as condições técnicas e ambientais para a instalação das soluções em no máximo 48 (quarenta e oito) horas úteis do recebimento da solicitação de serviço para implantação da solução;
- c) Implantar todos os softwares e hardwares necessários à prestação dos serviços de monitoração, gerência e administração remota da segurança, conforme as especificações técnicas constantes do Termo de Referência;
- d) Todas as soluções de hardware e software, ambientes de gerenciamento e monitoramento devem ser fornecidos em regime de locação;
- e) Iniciar a prestação dos serviços dentro dos prazos estabelecidos;
- f) As implantações das soluções serão realizadas pela CONTRATADA e todas as atividades envolvidas serão acompanhadas e coordenadas por analistas e técnicos da CONTRANTE;
- g) A CONTRATADA na implantação da solução, quando realizada no ambiente de produção, deverá ter a disponibilidade para executar determinadas atividades após o expediente (horários noturnos ou em finais de semana e feriados);
- h) A CONTRATADA deverá fornecer às senhas de configuração dos equipamentos, se existirem, a CONTRANTE, onde designará três pessoas para terem acesso a(s) senha(s), que devem ser fornecidas de forma segura. A CONTRANTE deverá seguir os procedimentos documentais acordados entre as partes, caso venha a fazer uso deste acesso, e se responsabilizará pelas consequências que por ventura possam advir deste acesso;
- i) A CONTRATADA será responsável por efetuar as atividades de integração da solução de monitoramento remoto com o ambiente operacional da CONTRANTE, sem prejuízo aos serviços desta;
- j) Registrar os tempos de atendimento dos chamados de suporte técnico ou chamados de serviços;
- k) Garantir e manter total e absoluto sigilo sobre as informações manuseadas, as quais devem ser utilizadas apenas para a condução das atividades autorizadas, não podendo ter quaisquer outros usos, sob pena de rescisão contratual e medidas cíveis e penais cabíveis, assumindo inteira responsabilidade pelo uso indevido ou ilegal de informações privilegiadas da CONTRANTE, praticado por seus empregados, conforme Acordo de Responsabilidade para Fornecedores, a ser assinado pela CONTRATADA no ato da assinatura do contrato;
- l) Não subcontratar parcialmente os serviços objeto do certame, com outra empresa, sem prévia anuência por escrito da contratante, sob pena de incorrer na rescisão do contrato;
- m) A CONTRATADA deverá disponibilizar, durante todo o período do contrato, todos os equipamentos e softwares necessários à execução dos serviços.

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

11.1. Não haverá exigência de garantia da execução contratual.

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

12.1. As sanções previstas nos artigos 155 e 163 da Lei nº 14.133/2021 e respectivos critérios sobre conduta e dosimetria, poderão ser aplicadas à Contratada, conforme detalhado nos próximos itens.

12.2. O Contratado será responsabilizado administrativamente pelas seguintes infrações:

- I. dar causa à inexecução parcial do contrato;
- II. dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;
- III. dar causa à inexecução total do contrato;
- IV. deixar de entregar a documentação exigida para o certame;
- V. não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;
- VI. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;
- VII. ensejar o retardamento da execução ou da entrega do objeto do Contrato sem motivo justificado.
- VIII. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a contratação ou na execução do contrato;
- IX. fraudar o credenciamento ou praticar ato fraudulento na execução do contrato;
- X. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- XI. praticar atos ilícitos com vistas a frustrar os objetivos da licitação;
- XII. praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

12.3. Serão aplicadas ao responsável pelas infrações administrativas previstas na Lei nº. 14.133/21, as seguintes sanções:

- a) Advertência, nas hipóteses do inciso I do item anterior que não acarretem prejuízos ao Contratante ou quando ocorrer execução insatisfatória, ou, ainda, na ocorrência de pequenos transtornos ao desenvolvimento da prestação dos serviços, desde que sua gravidade não recomende a aplicação de uma das sanções previstas nas alíneas “d”, “e” e “f” a seguir. (Inciso I do Art. 156 da Lei 14.133/21).
- b) Multa moratória por dia de atraso injustificado no cumprimento da obrigação contratual, proporcional ao item em atraso e nas seguintes condições (art. 162 da Lei 14.133/21):
 - b.1). Atraso em até 10 dias, multa moratória de 3%.
 - b.2). Atraso entre 11 e 20 dias, multa moratória de 5%.
 - b.3). Após decorrido o prazo de 20 dias, o fiscal do contrato deverá aplicar uma das sanções previstas nas alíneas “d”, “e” ou “f”.
 - b.4). Os prazos previstos nas alíneas b.1, b.2 e b.3, poderão ser suspensos, caso a Contratada, tempestivamente, justifique de forma plausível o atraso, e o fiscal do contrato, em não havendo prejuízos ao Contratante, aceite prorrogar o prazo de entrega, não podendo ser superior a metade do que foi inicialmente contratado. Após decorrido esse prazo, se iniciará automaticamente a contagem da multa moratória.
- c) A aplicação de multa de mora não impedirá que a Administração a converta em compensatória e promova a extinção unilateral do contrato com a aplicação cumulada de outras sanções previstas nesta Lei.
- d) Multa compensatória de até 10% do valor do contrato licitado ou celebrado com contratação direta e será aplicada ao responsável por qualquer das infrações administrativas previstas neste instrumento. (Inciso II e §3º do Art. 156 da Lei 14.133/21).
- e) Suspensão temporária do direito de participar em licitação e impedimento de contratar com a Contratante na hipótese do inciso II do item 12.2, por prazo não superior a 2 (dois) anos.

f) Impedimento de licitar e contratar com a Assembleia Legislativa do Tocantins, nas hipóteses dos incisos II, III, IV, V, IV e VII do item 12.2, quando não se justificar a imposição de penalidade mais grave, por prazo não superior a 3 (três) anos. (§4º do Art. 156 da Lei 14.133/21).
g) Declaração de inidoneidade para licitar ou contratar com todos os órgãos e entidades da Administração Pública direta e indireta da União, dos Estados, do Distrito Federal e dos Municípios, nas hipóteses dos incisos II, III, IV, V, IV e VII do item 12.2, quando se justificar a imposição de penalidade mais grave que a sanção referida no item “e”, bem como pelas infrações administrativas previstas nos incisos VIII, IX, X, XI e XII do item 12.2, pelo prazo de 3 (três) até 5 (cinco) anos. (§5º do Art. 156 da Lei 14.133/21).

12.4. A aplicação das sanções previstas nas alíneas “d”, “e” e “f” não acarretará automaticamente a rescisão dos contratos já firmados com o Contratante ou em curso de execução.

12.5. As sanções previstas nas alíneas “d”, “e” e “f”, poderão ser aplicadas juntamente com as da alínea “c”. Será facultada a defesa prévia do interessado, no respectivo processo, no prazo de 05 (cinco) dias úteis, para as sanções das alíneas “d” e “e” e 10 (dez) dias corridos para as sanções da alínea “f”.

12.6. Antes da aplicação de qualquer sanção será garantido ao licitante o contraditório e a ampla defesa em processo administrativo.

12.7. Os valores das multas deverão ser recolhidos junto ao Tesouro Estadual, em guia específica, no prazo estabelecido no documento, sendo cobrada judicialmente caso ocorra sua inadimplência.

12.8. As penalidades aqui previstas não serão aplicadas quando o descumprimento do estipulado no contrato ou no Edital decorrer de justa causa ou impedimento, devidamente comprovado e aceito pela Contratante.

12.9. Situações agravantes:

a) As sanções indicadas poderão ser majoradas em 50% para cada agravante até o limite de 60 (sessenta) meses, se ocorrer uma das situações a seguir:

a.1. Reincidência: Quando o licitante/Contratado já possuir registro de penalidade aplicada no âmbito da esfera estadual pela prática de qualquer das condutas tipificadas nos itens “d”, “e” e “f”, nos 12 (doze) meses anteriores ao fato que decorrerá a aplicação de nova penalidade.

a.2. Notória impossibilidade de atendimento ao edital: Quando comprovadamente o licitante desclassificado ou inabilitado não detinha condições de atender ao exigido em edital.

a.3. Deliberado não atendimento de diligências: Quando de forma deliberada (intencional) o licitante não atender ou responder solicitações relacionadas a diligências destinadas ao esclarecimento ou complementação da instrução do processo licitatório.

a.4. Declaração falsa de tratamento diferenciado: Quando comprovadamente o licitante apresentar declaração falsa de que possui direito à tratamento diferenciado previsto em legislação específica.

12.10. Situações atenuantes:

a) As penas previstas nos incisos IV, VI, VIII, poderão ser reduzidas em 50% (uma única vez) após a incidência do previsto na alínea “f”, quando não houver nenhum dano à Administração, em decorrência dos seguintes atenuantes:

a.1. Falha perdoável: Quando a conduta praticada pelo licitante ou contratado for comprovadamente decorrente de falha escusável.

a.2. Vícios alheios à conduta do particular: Quando a conduta praticada for decorrente da apresentação de documentação que contenha vícios ou omissões para os quais não tenha contribuído o licitante/Contratado; ou que não sejam de fácil identificação, devidamente comprovado.

a.3. Documentação equivocada que não atende ao edital, com ausência de dolo: Quando a conduta praticada pelo licitante/Contratado decorrer da apresentação de documentação que não atende às exigências do edital, desde que evidenciado equívoco no seu encaminhamento e não existir dolo na referida conduta.

12.11. A aplicação das penas previstas no presente item, que trata sobre as sanções, não exclui outras sanções previstas no edital, contrato ou na legislação vigente, sem prejuízo das responsabilidades civil e criminal dos envolvidos, inclusive perdas e danos causados para a Administração.

12.12. Para a apuração dos fatos e das condutas praticadas, baseada no princípio da boa-fé objetiva, a Administração poderá promover diligências visando o esclarecimento de dúvidas e a apuração da veracidade das informações, bem como considerar todas as provas e documentos apresentados pela defesa dos envolvidos.

12.13. Diligências poderão ser, inclusive, requisitadas pelo acusado, o qual terá direito ao contraditório e à ampla defesa, juntando ao processo todo meio de prova necessário à sua defesa.

CLÁUSULA DÉCIMA-TERCEIRA – DA ALTERAÇÃO SUBJETIVA

13.1 É admissível a fusão, cisão ou incorporação da CONTRATADA com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

CLÁUSULA DÉCIMA- QUARTA - DA PROTEÇÃO DE DADOS PESSOAIS

14.1 A prestação dos serviços objeto deste Termo, na modalidade de Infraestrutura como Serviço (IaaS), deverá observar, obrigatoriamente, as disposições da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente no que se refere à proteção, segurança e sigilo de dados eventualmente tratados, armazenados ou processados em virtude da execução contratual.

14.2. A empresa contratada deverá:

14.2.1. Assegurar a implementação de medidas técnicas e administrativas adequadas à proteção dos dados pessoais armazenados ou trafegados por meio da infraestrutura contratada, protegendo-os contra acessos não autorizados, perda, destruição, alteração, vazamento ou qualquer forma de tratamento inadequado ou ilícito;

14.2.2. Garantir a confidencialidade, integridade e disponibilidade dos dados, bem como a rastreabilidade das ações executadas na infraestrutura, por meio de controles de acesso, registros de log e demais ferramentas de auditoria e monitoramento compatíveis com boas práticas de segurança da informação;

14.2.3. Preferencialmente, disponibilizar infraestrutura com data centers localizados em território nacional, ou, alternativamente, em países que ofereçam nível de proteção de dados pessoais adequado, conforme definido pela Autoridade Nacional de Proteção de Dados (ANPD);

14.2.4. Comprometer-se a notificar imediatamente a Aleto em caso de incidente de segurança que possa comprometer dados pessoais tratados no âmbito do contrato;

14.2.5. Não compartilhar dados pessoais com terceiros sem autorização prévia e expressa da Aleto, salvo por força de obrigação legal;

14.2.6. Cooperar com a Administração Pública para garantir os direitos do titular de dados, inclusive mediante fornecimento de informações e apoio a eventuais auditorias ou fiscalizações promovidas pela Aleto ou por órgãos de controle.

14.2.7. O descumprimento das obrigações acima será considerado infração contratual grave, sujeita às penalidades previstas na legislação aplicável, sem prejuízo das responsabilidades civis, administrativas e penais cabíveis.

CLÁUSULA DÉCIMA QUINTA - DA ANTICORRUPÇÃO

15.1. Para execução do presente instrumento a CONTRATANTE e a CONTRATADA deverão observar o disposto na Lei 12.846/2013, regulamentada pelo Decreto Federal nº 8.420/2015.

15.2. Fica vedado aos licitantes e à Aleto oferecer, dar ou se comprometer a dar a quem quer que seja, ou aceitar ou se comprometer a aceitar de quem quer que seja, tanto por conta própria quanto através de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou não financeiras ou benefícios de qualquer espécie que constituam prática ilegal ou de corrupção sob as leis de qualquer país, seja de forma direta ou indireta quanto ao objeto deste contrato, ou de outra forma que não relacionada a este contrato, devendo garantir, ainda, que seus prepostos e colaboradores ajam da mesma forma e observando sempre a legislação pertinente.

CLÁUSULA DÉCIMA SEXTA - DA EXTINÇÃO CONTRATUAL (art. 92, XIX)

16.1. Constituirão motivos para extinção do contrato, a qual deverá ser formalmente motivada nos autos do processo, assegurados o contraditório e a ampla defesa, as seguintes situações:

- I - não cumprimento ou cumprimento irregular de normas editalícias ou de cláusulas contratuais, de especificações dos serviços, ou de prazos;
- II - desatendimento das determinações regulares emitidas pela autoridade designada para acompanhar e fiscalizar sua execução ou por autoridade superior;
- III - alteração social ou modificação da finalidade ou da estrutura da empresa que restrinja sua capacidade de concluir o contrato;
- IV - decretação de falência ou de insolvência civil, dissolução da sociedade ou falecimento do contratado;
- V - caso fortuito ou força maior, regularmente comprovados, impeditivos da execução do contrato;
- VI - razões de interesse público, justificadas pela autoridade máxima do órgão ou da entidade contratante.

16.2. O contratado terá direito à extinção do contrato nas seguintes hipóteses:

- I - supressão, por parte da Administração, de serviços que acarrete modificação do valor inicial do contrato além do limite permitido no art. 125 da Lei 14.133/2021;
- II - suspensão de execução do contrato, por ordem escrita da Administração, por prazo superior a 03 (três) meses;
- III - repetidas suspensões que totalizem 90 (noventa) dias úteis, independentemente do pagamento obrigatório de indenização pelas sucessivas e contratualmente imprevistas desmobilizações e mobilizações e outras previstas;
- IV - atraso superior a 02 (dois) meses, contado da emissão da nota fiscal, dos pagamentos ou de parcelas de pagamentos devidos pela Administração por despesas de serviços.

16.3. As hipóteses de extinção a que se referem os subitens II, III e IV observarão as seguintes disposições:

- I - não serão admitidas em caso de calamidade pública, de grave perturbação da ordem interna ou de guerra, bem como quando decorrerem de ato ou fato que o contratado tenha praticado, do qual tenha participado ou para o qual tenha contribuído;
- II - assegurarão ao contratado o direito de optar pela suspensão do cumprimento das obrigações assumidas até a normalização da situação, admitido o restabelecimento do equilíbrio econômico-

financeiro do contrato, na forma da alínea d do inciso II do caput do art. 124 da Lei nº 14.133/2021.

16.4 Os emitentes das garantias previstas para a presente contratação deverão ser notificados pelo contratante quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

16.5. A extinção do contrato poderá ser:

I - determinada por ato unilateral e escrito da Administração, exceto no caso de descumprimento decorrente de sua própria conduta;

II - consensual, por acordo entre as partes, por conciliação, por mediação ou por comitê de resolução de disputas, desde que haja interesse da Administração;

III - determinada por decisão arbitral, em decorrência de cláusula compromissória ou compromisso arbitral, ou por decisão judicial.

16.5.1. A extinção determinada por ato unilateral da Administração e a extinção consensual deverão ser precedidas de autorização escrita e fundamentada da autoridade competente e reduzidas a termo no respectivo processo.

16.5.2 Quando a extinção decorrer de culpa exclusiva da Administração, o contratado será ressarcido pelos prejuízos regularmente comprovados que houver sofrido e terá direito a:

I - devolução da garantia;

II - pagamentos devidos pela execução do contrato até a data de extinção;

III - pagamento do custo da desmobilização.

16.6. A extinção determinada por ato unilateral da Administração poderá acarretar, sem prejuízo das sanções previstas na Lei 14.133/2021, as seguintes consequências:

I - execução da garantia contratual para:

a) ressarcimento da Administração Pública por prejuízos decorrentes da não execução;

b) pagamento de verbas trabalhistas, fundiárias e previdenciárias, quando cabível;

c) pagamento das multas devidas à Administração Pública;

d) exigência da assunção da execução e da conclusão do objeto do contrato pela seguradora, quando cabível;

II - retenção dos créditos decorrentes do contrato até o limite dos prejuízos causados à Administração Pública e das multas aplicadas.

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

17.1. As despesas decorrentes da presente contratação correrão à conta de recursos próprios da Assembleia Legislativa do Tocantins, consignados no seu Orçamento deste exercício, na dotação abaixo discriminada:

xxxxxxxxxxxxxxxxxx

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

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

CLÁUSULA DÉCIMA NONA – ALTERAÇÕES CONTRATUAIS

19.1. O contrato poderá ser alterado, com as devidas justificativas, nos seguintes casos:

I - unilateralmente pela Administração;

a) quando houver modificação do projeto ou das especificações, para melhor adequação técnica a seus objetivos;

b) quando for necessária a modificação do valor contratual em decorrência de acréscimo ou diminuição quantitativa de seu objeto, nos limites permitidos pela Lei 14.133/2021.

II - por acordo entre as partes:

a) quando conveniente a substituição da garantia de execução;

b) quando necessária a modificação do regime de execução do serviço, em face de verificação técnica da inaplicabilidade dos termos contratuais originários;

c) quando necessária a modificação da forma de pagamento por imposição de circunstâncias supervenientes, mantido o valor inicial atualizado e vedada a antecipação do pagamento em relação ao cronograma financeiro fixado, sem a correspondente contraprestação da execução do serviço;

d) para restabelecer o equilíbrio econômico-financeiro inicial do contrato em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução do contrato tal como pactuado, respeitada, em qualquer caso, a repartição objetiva de risco estabelecida no contrato.

19.2. Nas alterações unilaterais, a que se refere o inciso I do caput do art. 124 da Lei 14.133/2021, o contratado será obrigado a aceitar, nas mesmas condições contratuais, acréscimos ou supressões que se fizerem nos serviços. de até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

19.2.1. As alterações unilaterais a que se refere o subitem acima, não poderão transfigurar o objeto da contratação.

19.3. Caso haja alteração unilateral do contrato que aumente ou diminua os encargos do contratado, a Administração deverá restabelecer, no mesmo termo aditivo, o equilíbrio econômico-financeiro inicial.

19.4. A extinção do contrato não configurará óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório.

19.5. O pedido de restabelecimento do equilíbrio econômico-financeiro deverá ser formulado durante a vigência do contrato e antes de eventual prorrogação nos termos do art. 107 da Lei nº 14.133/2021.

19.6. A formalização do termo aditivo é condição para a execução, pela contratada, das prestações determinadas pela Administração no curso da execução do contrato, salvo nos casos de justificada necessidade de antecipação de seus efeitos, hipótese em que a formalização deverá ocorrer no prazo máximo de 01 (um) mês.

19.7. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, como nas seguintes situações:

I - variação do valor contratual para fazer face ao reajuste de preços previstos no próprio contrato;

II - atualizações, compensações ou penalizações financeiras decorrentes das condições de pagamento previstas no contrato;

III - alterações na razão ou na denominação social do contratado;

IV - empenho de dotações orçamentárias.

CLÁUSULA VIGÉSIMA – PUBLICAÇÃO DO CONTRATO

20.1. Incumbirá à contratante divulgar o presente instrumento, na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo sítio oficial na Internet, em atenção ao art. 91, caput, da Lei n.º 14.133, de 2021, e ao art. 8º, §2º, da Lei n. 12.527, de 2011.

CLÁUSULA VIGÉSIMA PRIMEIRA - DO FORO

21.1. As questões decorrentes da execução deste Instrumento, que não possam ser dirimidas administrativamente, serão processadas e julgadas na Justiça Estadual, no Foro de Palmas - TO, com exclusão de qualquer outro, por mais privilegiado que seja.

Fica expressamente vedada a vinculação deste Contrato em operação de qualquer natureza que a CONTRATADA tenha ou venha a assumir.

E, para firmeza e validade do que foi pactuado, lavrou-se o presente Contrato em 02 (duas) vias de igual teor e forma, para que surtam um só efeito, às quais, depois de lidas, são assinadas pelos representantes das partes CONTRATANTE e CONTRATADA.

Palmas (TO), ____ de _____ 2025.

CONTRATANTE

XXXXXXXXXX

CONTRATADA

XXXXXXXXXXXXXXXXXXXXXXXXXXXX

1ª. Testemunha

2ª. Testemunha