



TRIBUNAL DE CONTAS DE RORAIMA
Rua Agnelo Bittencourt nº 126, - Bairro Centro, Boa Vista/RR, CEP 69301-430
Telefone: (95) 2121-4444 - <http://www.tcerr.tc.br>

EDITAL Nº 22/2025

Processo nº 002350/2025

LICITAÇÃO Nº 022/2025- PREGÃO ELETRÔNICO

O Tribunal de Contas do Estado de Roraima, por intermédio da Comissão de Contratação, nomeada pela portaria nº 1047/2025/TCERR, torna público que **REALIZARÁ LICITAÇÃO NA MODALIDADE PREGÃO, NA FORMA ELETRÔNICA**, nos termos da Lei N.º 14.133/2021, Resolução nº 021/2023-TCERR-PLENO, Resolução nº 002/2024 - TCERR-PLENO e demais legislações aplicáveis e pelas condições e exigências constantes do presente Edital e em conformidade com a autorização contida no Processo SEI nº 002350/2025.

OBJETO:

O objeto da presente licitação é a escolha da proposta mais vantajosa, cujo objeto é a **Contratação de serviços de gerenciamento de Firewall de Borda, WAF (Web Application Firewall) e SOC (Security Operations Center), incluindo suporte técnico remoto e especializado, para atendimento à infraestrutura de tecnologia da informação do Tribunal de Contas do Estado de Roraima (TCERR)**, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

A licitação será por **GRUPO**, contendo dois ou mais itens, conforme tabela constante do item 4 - Anexo I - Termo de Referência.

CRITÉRIO DE JULGAMENTO:

O critério de julgamento adotado será o **MENOR PREÇO**, observadas as exigências contidas neste Edital e seus Anexos quanto às especificações do objeto.

DA SESSÃO PÚBLICA DO PREGÃO ELETRÔNICO

Abertura da sessão: **06/01/2026 às 10h00min (horário de BRASÍLIA/DF)**

ENDEREÇO ELETRÔNICO: <https://www.gov.br/compras/pt-br>

Código UASG: 925458

E-mail: cpl@tcerr.tc.br

NOME INSTITUCIONAL: TRIBUNAL DE CONTAS DO ESTADO DE RORAIMA - CNPJ nº 84.008.440/0001-85.

Fazem parte integrante deste EDITAL, para todos os fins e efeitos, os seguintes anexos:

ANEXO I – Termo de Referência;

ANEXO II – Modelo de apresentação da proposta de preços;

ANEXO II - A -Tabela de Correlação de Requisitos do Termo de Referência e Proposta Técnica (Ponto a Ponto).

ANEXO III – Modelo de declaração de inexistência de práticas de nepotismo;

ANEXO IV – Minuta de Instrumento de Contrato;

1. PREÂMBULO

1.1. A abertura da presente licitação dar-se-á em sessão pública, e será aberta automaticamente pelo sistema eletrônico (comunicação pela Internet), dirigida pelo Pregoeiro, a ser realizada conforme indicado a seguir, de acordo com a legislação referida no preâmbulo deste Edital. Todas as referências de tempo neste Edital, no aviso e durante a sessão pública observarão obrigatoriamente o **horário de Brasília/DF** e, desta forma, serão registradas no sistema eletrônico e na documentação relativa ao certame.

1.2. As propostas deverão ser enviadas a partir da data de início do acolhimento no sistema eletrônico até o horário limite da abertura da sessão.

1.3. Eventualmente, não havendo expediente na data marcada, ficará a reunião adiada para o primeiro dia útil subsequente, mantidos o mesmo horário e endereço eletrônico anteriormente estabelecido, desde que não haja comunicação do Pregoeiro(a) em contrário.

1.4. Este edital será publicado na forma da lei e estará à disposição dos interessados, pela internet, nos endereços <https://www.gov.br/compras/pt-br> e www.tcerr.tc.br (menu “LICITAÇÕES”), no **Portal Nacional de Contratações Públicas (PNCP)** e poderá ser obtido, ainda, sem ônus, junto ao Pregoeiro ou à Equipe de apoio, em mídia digital, no Edifício sede do Tribunal de Contas do Estado de Roraima, sito na Rua Professor Agnelo Bittencourt, 126 – Centro, Boa Vista/Roraima, térreo, Comissão Permanente de Licitação - CPL, no horário de 8h 30min às 14h 30min (horário de Brasília/DF), devendo aos interessados a entrega do CD-R ou *pen-drive* para que seja providenciada a gravação.

2. DOS RECURSOS ORÇAMENTÁRIOS

2.1. A despesa decorrente da presente contratação correrá por conta da seguinte dotação:

- **Unidade Gestora:** Tribunal de Contas do Estado de Roraima
- **Projeto de Trabalho:** 01.032.002.2012.9900.
- **Fonte (s):** 1500.
- **Natureza da Despesa:** 3.3.90.40 – Serviços de Tecnologia da Informação e Comunicação.

3. DO PREÇO MÁXIMO

3.1. O preço estimado é valor obtido por método matemático aplicado em série de preços coletados, desconsiderando-se, na sua composição, os valores inexequíveis e os excessivamente elevados, de acordo com o que dispõe o inciso X da Resolução nº 017/2023-TCERR-PLENO.

4. DAS CONDIÇÕES PARA PARTICIPAÇÃO

4.1. Poderão participar deste Pregão os interessados que estiverem previamente credenciados perante o sistema eletrônico provido pela Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão (SLTI), por meio do sítio <https://www.gov.br/compras/pt-br/>

4.2. Para ter acesso ao sistema eletrônico, os interessados em participar deste Pregão deverão dispor de chave de identificação e senha pessoal, obtidas junto à SLTI, onde também deverão informar-se a respeito do seu funcionamento e regulamento e receber instruções detalhadas para sua correta utilização.

4.3. 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.

4.4. O uso da senha de acesso pela licitante é de sua responsabilidade exclusiva, incluindo qualquer transação por ele efetuada diretamente, ou por seu representante, não cabendo ao provedor do sistema ou ao TCERR, responsabilidade por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros.

4.5. Não poderão disputar esta licitação:

4.5.1. pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar em decorrência de sanção que lhe foi imposta, no âmbito da sanção;

4.5.2. 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, devendo essa proibição constar expressamente do edital de licitação;

4.5.3. empresas controladoras, controladas ou coligadas, nos termos da [Lei nº 6.404, de 15 de dezembro de 1976](#), concorrendo entre si;

4.5.4. 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.

4.5.4.1. O impedimento de que trata o item 4.5.1, será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

4.5.5. 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.

4.5.6. empresas cujo estatuto ou contrato social não seja pertinente e compatível com o objeto desta licitação.

4.5.7. empresas em processo de falência;

4.5.8. empresas estrangeiras não autorizadas a funcionar no país.

4.5.9. Não será permitida a partição de pessoa jurídica constituída por meio de **consórcio**, em razão do baixo valor e da baixa complexidade do objeto, sob pena de perder a economia de escala.

4.5.10. Não será permitida a participação de **Cooperativas** no presente certame em razão da incompatibilidade da forma de execução/metodologia dos serviços objeto deste termo com a forma de funcionamento das Cooperativas conforme previsto na Lei nº 12.690/2012.

5. DOS ESCLARECIMENTOS E DA IMPUGNAÇÃO AO EDITAL

5.1. Qualquer pessoa é parte legítima para impugnar edital de licitação por irregularidade ou para solicitar esclarecimento sobre os seus termos, devendo encaminhar o pedido até 3 (três) dias úteis antes da data de abertura da sessão pública, por meio eletrônico, na forma prevista no edital de licitação.

5.2. O Pregoeiro responderá aos pedidos de esclarecimentos e/ou impugnação no prazo de até 3 (três) dias úteis contado da data de recebimento do pedido, limitado ao último dia útil anterior à data da abertura do certame, e poderá requisitar subsídios formais aos responsáveis pela elaboração do edital de licitação e dos anexos.

5.3. A resposta ao pedido de esclarecimento não deve ser utilizada para fins de retificar os termos do edital e/ou seus anexos no curso do procedimento, devendo, nesse caso, ser avaliada criteriosamente pelo Pregoeiro, se a questão levantada pelo interessado tem força de alterar cláusula editalícia que afete a formulação das propostas das licitantes, em especial quando a resposta for subsidiada pela manifestação de unidade técnica, observando-se o contido §1º do art. 55 da Lei 14.133/2021.

5.4. Na análise da impugnação, o Pregoeiro tem o dever de diligenciar, especialmente quando for apontada cláusula editalícia restritiva da competitividade, devendo realizar a revisão criteriosa do instrumento convocatório, ainda que a impugnação não seja tempestiva.

5.5. A impugnação não possui efeito suspensivo, sendo a sua concessão medida excepcional que deverá ser motivada pelo Pregoeiro, nos autos do processo de licitação.

5.6. Acolhida a impugnação contra o edital de licitação, será definida e publicada nova data para realização do certame, observados os prazos fixados no art. 16 da Resolução nº 021/2023 TCERR-PLENO.

5.7. As respostas aos pedidos de esclarecimentos e as impugnações serão divulgadas em sítio eletrônico do TCERR e no sistema, dentro do prazo estabelecido no item 5.1. e vincularão os participantes e o Tribunal de Contas do Estado de Roraima.

6. DA APRESENTAÇÃO DA PROPOSTA DE PREÇOS

6.1. Após a divulgação do edital de licitação, os licitantes encaminharão, exclusivamente por meio do sistema, a proposta de preço, até a data e o horário estabelecidos para abertura da sessão pública.

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

6.2.1. O cumprimento dos requisitos para a habilitação e a conformidade de sua proposta com as exigências

do edital de licitação e que está ciente e concorda com as condições contidas neste 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 ainda, as declarações abaixo:

6.2.2. 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;

6.2.3. 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;

6.2.4. 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.

6.3. O fornecedor enquadrado como microempresa, empresa de pequeno porte deverá declarar, ainda, 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.

6.4. A falsidade das declarações de que trata o item 6.2.1, sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021.

6.5. Os licitantes poderão retirar ou substituir a proposta até a abertura da sessão pública.

6.6. 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.

6.7. 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.

6.8. 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

6.9. Quando do cadastramento da proposta, na forma estabelecida no item 6.1. o licitante poderá parametrizar o seu valor final mínimo e obedecerá às seguintes regras:

6.9.1. 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;

6.9.2. os lances serão de envio automático pelo sistema, respeitado o valor final mínimo estabelecido e o intervalo de que trata o item 6.10.1.

6.10. O valor final mínimo de que trata o item 6.9. poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:

6.10.1. valor superior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por menor preço.

6.11. O valor final mínimo parametrizado na forma do item 6.9. possuirá caráter sigiloso para os demais fornecedores e para o promotor da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de Controle Externo e Interno.

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

6.12.1 Valor total do contrato de acordo com o prazo de vigência, conforme Anexo I - Termo de Referência.

6.12.2. Descrição do objeto, contendo as informações conforme as especificações constantes do Anexo I - Termo de Referência, em conformidade com o ANEXO II – Modelo de Proposta de Preços.

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

6.13. 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.

6.14. 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.

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

6.16. 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.

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

6.18. O licitante **não** poderá oferecer proposta em quantitativo inferior ao máximo previsto para contratação.

6.19. Os licitantes devem respeitar os preços máximos previstos no Termo de Referência, considerando o critério de menor preço.

7. DA ABERTURA DA SESSÃO PÚBLICA E DA CLASSIFICAÇÃO DAS PROPOSTAS.

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. Será desclassificada a proposta que identifique o licitante.

7.4. A desclassificação será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

7.5. A não desclassificação da proposta não impede o seu julgamento definitivo em sentido contrário, levado a efeito na fase de aceitação.

7.6. O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.

7.7. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes, sendo vedada outra forma de comunicação.

8. DO MODO DE DISPUTA E FORMULAÇÃO DE LANCES

8.1. Iniciada a etapa competitiva, observado o modo de disputa adotado neste Edital, os licitantes deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

8.2. O lance deverá ser ofertado pelo valor total global, conforme prazo de vigência disposto no Anexo I - Termo de Referência.

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

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

8.5. 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 R\$ 1,00 (um real).

8.6. O modo de **disputa "aberto"**, a etapa de envio de lances durará **10 (dez) minutos** e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos **2 (dois) minutos** do período de duração desta etapa.

8.6.1. A prorrogação automática da etapa de envio de lances, de que trata o item 8.6, será de 2 (dois) minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive quando se tratar de lances intermediários.

8.6.2. Após a etapa de que trata o item 8.6.1., o sistema abrirá a oportunidade para que o autor da oferta de valor mais baixo ou de maior percentual de desconto e os autores das ofertas subsequentes com valores ou percentuais até 10% (dez por cento) superiores ou inferiores àquela, conforme o critério adotado, possam ofertar um lance final e fechado em até 5 (cinco) minutos, que será sigiloso até o encerramento deste prazo.

8.6.3. No procedimento de que trata o item 8.6.2., o licitante poderá optar por manter o seu último lance da etapa aberta, ou por ofertar melhor lance.

8.6.4. Na ausência de, no mínimo, 3 (três) ofertas nas condições de que trata o item 8.6.2, os autores dos

melhores lances subsequentes, na ordem de classificação, até o máximo de 3 (três), poderão oferecer um lance final e fechado em até 5 (cinco) minutos, que será sigiloso até o encerramento do prazo, observado o disposto no item 8.6.3.

8.6.5. Encerrados os prazos estabelecidos nos itens 8.6.2. e 8.6.4, os lances serão ordenados pelo sistema e divulgados da seguinte forma:

- a) ordem crescente, quando adotado o critério de julgamento por menor preço; ou
- b) ordem decrescente, quando adotado o critério de julgamento por maior desconto.

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

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

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

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

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

8.12. Após a fase de lances, se a proposta mais bem classificada não tiver sido apresentada por microempresa ou empresa de pequeno porte, e houver proposta de microempresa ou empresa de pequeno porte que seja igual ou até 5% (cinco por cento) superior à proposta mais bem classificada, proceder-se-á da seguinte forma:

8.12.1 A microempresa ou a empresa de pequeno porte mais bem classificada poderá, no prazo de 5 (cinco) minutos, contados do envio da mensagem automática pelo sistema, apresentar uma última oferta, obrigatoriamente inferior à proposta do primeiro colocado, situação em que, atendidas as exigências habilitatórias e observado o valor máximo para a contratação, será adjudicado em seu favor o objeto deste Pregão;

8.12.2 Não sendo vencedora a microempresa ou a empresa de pequeno porte mais bem classificada, na forma do subitem anterior, o sistema, de forma automática, convocará as licitantes remanescentes que porventura se enquadrem na situação descrita nesta condição, na ordem classificatória, para o exercício do mesmo direito;

8.13. No caso de equivalência dos valores apresentados pelas microempresas ou empresas de pequeno porte que se encontrem no intervalo estabelecido nesta condição, o sistema fará um sorteio eletrônico, definindo e convocando automaticamente a vencedora para o encaminhamento da oferta final do desempate;

8.14. A empresa convocada que não apresentar proposta dentro do prazo de 5 (cinco) minutos, controlados pelo sistema, decairá do direito previsto nos artigos 44 e 45 da Lei Complementar n.º 123/2006.

8.15. Não ocorrendo adjudicação, nos termos previstos no subitem 8.16, o objeto licitado será adjudicado em favor da licitante detentora da proposta originalmente melhor classificada, se houver compatibilidade de preço com o valor de referência e a licitante for considerada habilitada

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

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

8.18. Esgotados todos os demais critérios de desempate previstos no item 8.17, a escolha do licitante vencedor ocorrerá por sorteio, em ato público, para o qual todos os licitantes serão convocados, vedado qualquer outro processo.

9. DA FASE DE JULGAMENTO

9.1. Encerrada a etapa de envio de lances da sessão pública, o Pregoeiro realizará a verificação da conformidade da proposta classificada em primeiro lugar quanto à adequação ao objeto do certame e, observado o disposto no art. 33 da Resolução nº 021/2023-TCERR-PLENO, à compatibilidade do preço em relação ao estimado para a contratação, conforme definido no edital.

9.2. Desde que previsto no edital, o Pregoeiro, em relação ao licitante provisoriamente vencedor, realizará análise e avaliação da conformidade da proposta, mediante homologação de amostras, exame de conformidade e prova de conceito, entre outros testes de interesse do Tribunal de Contas do Estado de Roraima de modo a comprovar sua aderência às especificações definidas no Termo de Referência ou no Projeto Básico.

9.3. O Pregoeiro solicitará envio da proposta de preços (**MODELO DO ANEXO II**), e, se necessário, dos documentos complementares, adequada ao último lance ofertado, no prazo **máximo de 3 (três) horas**, prorrogável por igual período, contado da solicitação.

9.3.1. A prorrogação de que trata o item anterior, poderá ocorrer nas seguintes situações:

I - por solicitação do licitante, mediante justificativa aceita pelo Pregoeiro; ou

II - de ofício, a critério do Pregoeiro, quando constatado que o prazo estabelecido não é suficiente para o envio dos documentos exigidos no edital para a verificação de conformidade de que trata o item 9.1.

9.4. O Pregoeiro poderá requerer auxílio técnico do demandante ou de unidade técnica para fins de análise de conformidade das especificações contidas na proposta selecionada com as especificações do objeto pretendido.

9.5. Na hipótese da proposta de o primeiro colocado permanecer acima do preço máximo definido para a contratação, o Pregoeiro poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

9.5.1. A negociação será realizada por meio do sistema e poderá ser acompanhada pelos demais licitantes.

9.5.2. Quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido para a contratação, a negociação poderá ser feita com os demais licitantes classificados, exclusivamente por meio do sistema, respeitada a ordem de classificação estabelecida no §2º do art. 21 da Resolução nº 021/2023-TCERR-PLENO, ou, em caso de propostas intermediárias empatadas, serão utilizados os critérios de desempate definidos no art. 27 da Resolução nº 021/2023-TCERR-PLENO.

9.5.3. Concluída a negociação, se houver, o resultado será registrado na ata da sessão pública, devendo esta ser anexada aos autos do processo de contratação.

9.6. Caso a proposta do licitante vencedor não atenda ao quantitativo total estimado para a contratação, poderá ser convocada a quantidade de licitantes necessária para alcançar o total estimado, respeitada a ordem de classificação, observado o preço da proposta vencedora.

9.7. É indício de inexecuibilidade as propostas de valores inferiores a 50% (cinquenta por cento) do valor orçado pelo Tribunal de Contas do Estado de Roraima.

9.7.1 A inexecuibilidade, na hipótese de que trata o item anterior, só será considerada após diligência do Pregoeiro que comprove:

I - que o custo do licitante ultrapassa o valor da proposta; e

II - inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

9.7.2. Se houver indícios de inexecuibilidade 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.

9.8. Encerrada a fase de julgamento, após a verificação de conformidade da proposta, o Pregoeiro verificará a documentação de habilitação do licitante conforme disposições contidas neste edital de licitação, observado o disposto no item 10 deste edital.

9.9. Encerrada a fase de julgamento da proposta, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

a) SICAF;

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

c) Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (<https://www.portalttransparencia.gov.br/sancoes/cnep>).

9.10. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei nº 8.429, de 1992.

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

9.12. Caso atendidas as condições de participação, será iniciado o procedimento de habilitação.

9.13. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o pregoeiro verificará se faz jus ao benefício, em conformidade com o item 6.3. deste edital.

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

9.15. Será desclassificada a proposta vencedora que:

9.15.1. conter vícios insanáveis;

9.15.2. não obedecer às especificações técnicas contidas no Anexo I - Termo de Referência;

9.15.3. apresentar preços inexecutáveis ou permanecerem acima do preço máximo definido para a contratação;

9.15.4. não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

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

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

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

9.15.7.1. O ajuste de que trata o item acima, se limita a sanar erros ou falhas que não alterem a substância das propostas;

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

9.15.9. 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

9.15.10. O Pregoeiro, poderá, no julgamento das propostas, sanar erros ou falhas que não alterem a sua substância e sua validade jurídica, atribuindo-lhes eficácia para fins de classificação, observado o disposto no art. 55 da Lei nº 9.784, de 29 de janeiro de 1999.

9.15.11. Cabe ao Pregoeiro indicar de forma clara e objetiva as inconsistências sanáveis na proposta e/ou planilhas apresentadas pelo licitante, sem alteração do valor declarado vencedor.

9.15.12. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento de que trata o item 9.15.10, o seu reinício somente poderá ocorrer mediante aviso prévio no sistema com, no mínimo, 24 (vinte e quatro) horas de antecedência, e a ocorrência será registrada em ata.

10. DA HABILITAÇÃO

10.1. Para habilitação dos licitantes, serão exigidos os documentos necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, nos termos dos arts. 62 a 70 da Lei nº 14.133, de 2021.

10.1.1. A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira, desde que previsto no edital de licitação, poderá ser substituída pelo registro cadastral no SICAF.

10.2. A habilitação das licitantes será verificada por meio do SICAF e da documentação complementar especificada neste Edital.

10.3. Os documentos exigidos para habilitação que não estejam contemplados no SICAF, serão enviados por meio do sistema, quando solicitado pelo Pregoeiro, até a conclusão da fase de habilitação.

10.4. As licitantes deverão apresentar a seguinte documentação complementar:

10.4.1. Habilitação Jurídica:

10.4.1.1. Empresário Individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

10.4.1.2. Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da sua autenticidade;

10.4.1.3. Sociedade Empresária, Sociedade Limitada Unipessoal – SLU ou sociedade identificada como Empresa Individual de Responsabilidade Limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva

sede, acompanhada de documento comprobatório de seus administradores;

10.4.1.4. Sociedade Empresária Estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede;

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

10.4.1.6. Filial, Sucursal ou Agência de Sociedade Simples ou Empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz;

10.4.1.7. Consórcio: Não será permitida a partição de pessoa jurídica constituída por meio de consórcio, em razão do baixo valor e da baixa complexidade do objeto, sob pena de perder a economia de escala.

10.4.1.8. Não será permitida a participação de **Cooperativas** no presente certame em razão da incompatibilidade da forma de execução/metodologia dos serviços objeto deste termo com a forma de funcionamento das Cooperativas conforme previsto na Lei nº 12.690/2012.

10.4.2. Habilitação Fiscal, Social e Trabalhista:

10.4.2.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas;

10.4.2.2. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão conjunta federal expedida pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional;

10.4.2.3. Prova de regularidade junto ao Fundo de Garantia do Tempo de Serviço (FGTS);

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

10.4.2.5. Prova de inscrição no cadastro de contribuintes estadual e/ou municipal relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

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

10.4.2.7. Declaração de Inexistência de Trabalho Infantil, em cumprimento do inciso XXXIII, da Constituição Federal.

10.4.2.8. Em se tratando de filial, os documentos de habilitação jurídica e regularidade fiscal deverão estar em nome da filial, exceto aqueles que, pela própria natureza, são emitidos somente em nome da matriz

10.4.2.9. Caso a licitante seja considerada isenta dos tributos estaduais ou municipais relacionados ao objeto da contratação, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda Estadual ou Municipal do seu domicílio ou sede, ou outra equivalente, na forma da lei.

10.4.2.10. O fornecedor ou prestador enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal, uma vez que o Certificado de Condição de Microempreendedor Individual – CCMEI supre as exigências de inscrição nos cadastros fiscais, na medida em que essas informações constam no próprio Certificado.

10.4.3. Qualificação Econômico-Financeira:

10.4.3.1. Certidão Negativa de Falência expedida pelo distribuidor da sede do fornecedor;

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

$$a) \text{ Liquidez Geral (LG)} = (\text{Ativo Circulante} + \text{Realizável a Longo Prazo}) / (\text{Passivo Circulante} +$$

Passivo Não Circulante);

b) *Solvência Geral (SG)* = *(Ativo Total)/(Passivo Circulante + Passivo não Circulante)*; e

c) *Liquidez Corrente (LC)* = *(Ativo Circulante)/(Passivo Circulante)*.

10.4.3.3. Empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências de habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura, nos termos do art. 65, §1º, da Lei 14.133/2021.

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

10.4.3.5. Os documentos acima referenciados deverão ser exigidos com base no limite definido pela **Receita Federal do Brasil** para transmissão da **Escrituração Contábil Digital - ECD** ao **SPED**.

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

10.4.4. Qualificação Técnica:

10.4.4.1. A licitante deverá apresentar Atestado de Capacidade Técnica ou documento equivalente, emitido por pessoa jurídica de direito público ou privado, comprovando a execução de serviços compatíveis com o objeto deste Termo de Referência.

10.4.4.2. A licitante deverá disponibilizar, quando solicitado pelo TCERR, informações que permitam comprovar a legitimidade dos atestados apresentados, incluindo, mas não se limitando a: cópia do contrato que deu origem à prestação dos serviços, endereço da contratante, local de execução do objeto e outros documentos julgados necessários para atestar a idoneidade do(s) atestado(s).

10.4.4.3. A habilitação da licitante poderá ser comprovada por meio do Sistema de Cadastro Unificado de Fornecedores (SICAF), nos documentos por ele abrangidos.

10.5. Após a apresentação dos documentos de habilitação, fica vedada a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para:

I - 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

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

III - suprir ausência de documento de cunho declaratório emitido unilateralmente pelo licitante.

10.6. Na hipótese de que trata o item 10.4, os documentos deverão ser apresentados em formato digital, via sistema, no prazo **máximo de 3 (três) horas**, após solicitação do Pregoeiro, no sistema eletrônico prorrogável por igual período, nas situações elencadas:

I - por solicitação do licitante, mediante justificativa aceita pelo Pregoeiro; ou

II - de ofício, a critério do Pregoeiro quando constatado que o prazo estabelecido não é suficiente para o envio dos documentos exigidos no edital para a verificação de conformidade de que trata o *caput* do art. 28.

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

10.8. Na análise dos documentos de habilitação, o Pregoeiro poderá sanar erros ou falhas, na forma estabelecida no Capítulo XI da Resolução **nº 021/2023-TCERR-PLENO**.

10.9. Na hipótese de o licitante não atender às exigências para habilitação, o Pregoeiro, examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao edital de licitação, observado o item 9.3. do edital.

10.10. Os documentos de habilitação deverão estar atualizados até a data da solicitação do Pregoeiro, após a fase de julgamento das propostas, apenas do licitante vencedor, conforme disposto no caput do art. 28 da Resolução **nº 021/2023-TCERR-PLENO**

10.11. Serão disponibilizados para acesso público os documentos de habilitação dos licitantes convocados para a apresentação da documentação habilitatória, após concluídos os procedimentos de que trata o item 10.8. do Edital.

10.12. A comprovação da regularidade fiscal e trabalhista das microempresas e das empresas de pequeno porte será exigida nos termos da legislação pertinente.

10.13 Para comprovação da inexistência de **práticas de nepotismo**, o licitante deverá apresentar, declaração de que não mantém vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do Contratante ou com servidor que desempenhe função no procedimento licitatório ou na contratação direta, bem como 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, conforme **MODELO do ANEXO III, deste Edital**.

11. RECURSOS

11.1. Qualquer licitante poderá, durante o prazo de 10 (dez) minutos, de forma imediata após o término do julgamento das propostas e do ato de habilitação ou inabilitação, em campo próprio do sistema, manifestar sua intenção de recorrer, sob pena de preclusão, ficando a autoridade superior autorizada a adjudicar o objeto ao licitante declarado vencedor.

11.1.1. As razões do recurso deverão ser apresentadas em momento único, em campo próprio no sistema, no prazo de 3 (três) dias úteis, contados a partir da data de intimação ou de lavratura da ata de habilitação ou inabilitação ou, na hipótese de adoção da inversão de fases prevista no §1º do art. 7º da Resolução nº **021/2023-TCERR-PLENO**, da ata de julgamento.

11.1.2. Os demais licitantes ficarão intimados para, se desejarem, apresentar suas contrarrazões, no prazo de 3 (três) dias úteis, contado da data de intimação pessoal ou de divulgação da interposição do recurso.

11.2. Será assegurado ao licitante vista dos elementos indispensáveis à defesa de seus interesses.

11.3. O acolhimento do recurso importará na invalidação apenas dos atos que não possam ser aproveitados.

11.4. Em hipótese alguma haverá rejeição sumária das razões de recursos, competindo ao Agente de Contratação apenas a análise dos pressupostos recursais antes do seu regular prosseguimento.

12. DA HOMOLOGAÇÃO

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

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

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

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

12.1.4. adjudicar o objeto e homologar a licitação.

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

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

12.2.2. Nos casos de anulação e revogação, deverá ser assegurada a prévia manifestação dos interessados.

13. DA CONVOCAÇÃO DO VENCEDOR

13.1. Após a homologação, o licitante vencedor será convocado para assinar o termo de contrato, ou aceitar ou retirar o instrumento equivalente, no prazo de 03 (três) dias úteis, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021, e em outras legislações aplicáveis.

13.1.1. O prazo de convocação poderá ser prorrogado 1 (uma) vez, por igual período, mediante solicitação da parte durante seu transcurso, devidamente justificada e desde que o motivo apresentado seja aceito pelo Tribunal de Contas do Estado de Roraima.

13.1.2. Na hipótese de o vencedor da licitação não assinar o contrato, ou não aceitar ou não retirar o instrumento equivalente no prazo e nas condições estabelecidas, outro licitante poderá ser convocado, respeitada a ordem de classificação, para celebrar a contratação, ou instrumento equivalente, nas condições propostas pelo licitante vencedor, sem prejuízo da aplicação das sanções previstas na Lei nº 14.133, de 2021, e em outras legislações aplicáveis.

13.1.3. Caso nenhum dos licitantes aceitar a contratação nos termos do item 13.1.2, o Tribunal de Contas do

Estado de Roraima, observados o valor estimado e sua eventual atualização nos termos do edital de licitação, poderá:

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

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

13.1.4. A recusa injustificada do adjudicatário em assinar o contrato, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido no instrumento convocatório caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades legalmente estabelecidas e à imediata perda da garantia da proposta em favor do Tribunal de Contas do Estado de Roraima.

13.1.5. A regra do do item 13.1.4, não se aplicará aos licitantes remanescentes convocados na forma do subitem 13.1.3.1.

14. DA SANÇÃO ADMINISTRATIVA

14.1. O licitante será responsabilizado administrativamente pelas seguintes infrações:

14.1.1. deixar de entregar a documentação exigida para o certame;

14.1.2. não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

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. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;

14.1.5. fraudar a licitação ou praticar ato fraudulento na execução do contrato;

14.1.6. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

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

14.1.8. praticar ato lesivo previsto no art. 5º da Lei 12.846/2013.

14.2. A sanção de **MULTA** será aplicada ao responsável, tomando como base o valor do contrato licitado, nas infrações administrativas abaixo relacionadas:

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

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

Multa: 10% (dez por cento).

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

Multa: 15% (quinze por cento).

d) apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;

e) fraudar a licitação ou praticar ato fraudulento na execução do contrato;

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

g) praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

h) praticar ato lesivo previsto no art. 5º da Lei 12.846/2013.

Multa: 20% (vinte por cento).

14.3. Será aplicada a sanção de **IMPEDIMENTO DE LICITAR E CONTRATAR** com o Tribunal de Contas do Estado de Roraima pelo prazo máximo de 3 (três) anos quando não se justificar a imposição de penalidade mais grave, no caso de cometimento das infrações previstas nos subitens 14.1.1 e 14.1.2 (Pena: 6 (seis) meses, contados da publicação do extrato da sanção no Diário Eletrônico do TCERR.) e subitem 14.1.3 (Pena: 2 (dois) anos, contados da publicação do extrato da sanção no Diário Eletrônico do TCERR).

14.4. Será aplicada a sanção de **DECLARAÇÃO DE INIDONEIDADE** que impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, no caso de cometimento das sanções previstas nos subitens 14.1.4 e 14.1.5 (Pena: 3 (três) anos, contados da publicação do

extrato da sanção no Diário Eletrônico do TCERR) e subitens 14.1.6., 14.1.7. e 14.1.8 (Pena: 6 (seis) anos, contados da publicação do extrato da sanção no Diário Eletrônico do TCERR).

14.5. Será aplicada a sanção de **declaração de inidoneidade** para licitar ou contratar com a Administração Pública direta e indireta, de todos os entes federativos, no caso de cometimento de qualquer das infrações indicadas no item 14.1, pelo prazo de 3 (três) anos, quando se justificar a imposição de penalidade mais grave.

15. DAS DISPOSIÇÕES FINAIS

15.1. A autoridade superior ou delegatário poderá revogar o procedimento licitatório de que trata este edital, por motivo de conveniência e oportunidade, e deverá anular por ilegalidade insanável, de ofício ou por provocação de terceiros, assegurada a prévia manifestação dos interessados.

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

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

15.3.1. Na hipótese da ilegalidade de que trata o 15.1, ser constatada durante a execução contratual, aplica-se o disposto no art. 147 da Lei nº 14.133, de 2021.

15.4. Este edital deverá ser lido e interpretado na íntegra, não sendo aceitas alegações de desconhecimento após a inserção da proposta no sistema eletrônico.

15.5. Os horários estabelecidos no edital de licitação, no aviso e durante a sessão pública observarão o horário de Brasília, Distrito Federal, inclusive para contagem de tempo e registro no sistema eletrônico e na documentação relativa ao certame.

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

15.7. 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.

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

15.9. 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.

15.10. 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.

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

15.12. Os casos omissos decorrentes da aplicação deste instrumento convocatório serão dirimidos pela Diretoria de Gestão Administrativa e Financeira, que poderá propor normas complementares e disponibilizar informações adicionais, em meio eletrônico.

Boa Vista - RR, 12 de dezembro de 2025.

AMÉLIO VALMIR MARTINI MACHADO

Diretor de Gestão Administrativa e Financeira

ANEXO I - DO EDITAL

TERMO DE REFERÊNCIA

1. OBJETO

Contratação de serviços de gerenciamento de Firewall de Borda, WAF (Web Application Firewall) e SOC (Security Operations Center), incluindo suporte técnico remoto e especializado, para atendimento à infraestrutura de tecnologia da informação do Tribunal de Contas do Estado de Roraima (TCERR).

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. A presente contratação fundamenta-se no **Estudo Técnico Preliminar - ETP** (ep. 1101306).

2.2. O objeto está contemplado no Plano Contratações Anual 2025 (ep. 1064494) sob a descrição **Firewall**, e no evento 1131140 como **Contratação de SOC e Serviços Técnicos Especializados (SOC)**. A contratação consta também na **Proposta Orçamentária 2025** (ep. 0958101) como **Serviço Firewall Novo**, vinculada ao elemento de despesa **33.90.40 – Serviços TIC (Pessoa Jurídica)**.

3. NATUREZA E ENQUADRAMENTO DO OBJETO**3.1. Natureza do objeto:**

Serviço ([art. 6º, inciso XI, da Lei 14.133/2021](#)).

3.2. Enquadramento/Categoria do objeto:

Bens e serviços comuns ([art. 6º, inciso XIII, da Lei 14.133/2021](#)).

4. DESCRIÇÃO DO OBJETO E VALOR ESTIMADO

4.1. Os produtos deste Termo, com especificações técnicas e valores, foram definidos com base em pesquisa de mercado junto a 23 (vinte e três) fornecedores (ep. 1131994), dos quais 6 (seis) propostas foram consideradas válidas (02 Firewall e 04 SOC), conforme demonstrado no Mapa Comparativo de Preços (ep. 1132263). Os preços do **Grupo 1 [Firewall]** foram calculados pelo preço médio e do **Grupo 2 [SOC]** pelo menor preço.

4.2. A metodologia assegura fidedignidade da estimativa de custos, atendimento à Lei nº 14.133/2021 e estabelece parâmetro orçamentário, não correspondendo ao valor final a ser pago, garantindo economicidade e compatibilidade com o mercado.

GRUPO 1 [FIREWALL]					
Item	Descrição dos Serviços	Unidade.	Quantidade	Valor Unitário R\$	Valor Total R\$
1	Serviço de Gerenciamento de Tecnologia de Segurança de Rede (UTM-NGFW) , garantia e suporte técnico pelo período de 60 meses , com disponibilidade de 2 equipamentos em regime de comodato	Serv./mês	60	14.757,50	885.450,00
2	Serviço de Gerenciamento de Tecnologia de Segurança de Rede Aplicação WEB (WAF - Web Application Firewall) , garantia e suporte técnico pelo período de 60 meses , com disponibilidade de equipamentos em regime de comodato.	Serv./mês	60	16.900,00	1.014.000,00
3	Solução de Relatoria , garantia e suporte técnico pelo período de 60 meses .	Serv./mês	60	3.750,00	225.000,00
4	Serviço de Implantação, Migração e Configuração.	Serv	1	37.000,00	37.000,00
5	Serviço de Treinamento de equipe técnica do Contratante.	Serv	1	27.000,00	27.000,00

6	Serviços Técnicos Especializados em Segurança da Informação (sob demanda)	UST	120	358,33	43.000,00
Preços Globais do GRUPO 01 R\$					2.231.450,00

Tabela 1 - Valor estimado de Firewall Grupo 1

GRUPO 2 [SOC]					
Item	Descrição dos Serviços	Unidade.	Quantidade	Valor Unitário R\$	Valor Total R\$
7	Serviço de SOC 24x7 com SIEM, período de 36 meses	Serv./mês	36	22.029,60	793.065,60
8	Serviços Técnicos Especializados (SOC) (sob demanda) pelo período de 36 meses .	UST	1080	282,75	305.370,00
Preços Globais do GRUPO 02 R\$					1.098.435,60

Tabela 2 - Valor Estimado de SOC Grupo 2

4.3. Será exigida a apresentação de uma Correlação de Requisitos do Termo de Referência (Anexo I) com a Proposta Técnica dos fornecedores (Ponto a Ponto), conforme o modelo indicado no **Anexo II**. Ressalta-se que esta exigência possui caráter meramente informativo e organizacional, não configurando requisito habilitatório. Seu objetivo é facilitar a análise do atendimento de cada requisito, promovendo maior transparência e padronização na avaliação das propostas.

5. INDICAÇÃO DE MARCA/MODELO

Não se aplica.

6. REGIME DE EXECUÇÃO

O objeto do presente termo será executado de forma indireta, sob o regime de **empreitada por preço global**.

7. FORMA DE EXECUÇÃO DO SERVIÇO

O fornecimento será realizado em duas etapas, organizadas em grupos distintos, conforme descrito a seguir.

7.1. Grupo 1 - FIREWALL (Itens 1 a 6):

7.1.1. Os prazos para execução do **Grupo 1** estão estabelecidos na tabela abaixo:

ETAPA	EVENTOS	PRAZO
ETAPA 1	- Entrega do Equipamento - Instalação física da solução	45 dias após a assinatura do contrato
ETAPA 2	- Reunião "Kick-off" - Levantamento de requisitos e configurações atuais - Levantamento do ambiente e projeto de migração dos dados	5 dias após ETAPA 1
ETAPA 3	- Implantação das configurações da Solução e Migração	15 dias após a ETAPA 2
ETAPA 4	- Treinamento	10 dias após a ETAPA 3

Tabela 3 - Requisitos Temporais Grupo 1

7.1.2. O software e as subscrições contratadas deverão ser fornecidos antes do final da Etapa 2.

7.2. Grupo 2 - SOC (Itens 7 e 8):

7.2.1. Os prazos para execução do **Grupo 2** estão estabelecidos na tabela abaixo:

ETAPA	EVENTOS	PRAZO
--------------	----------------	--------------

ETAPA 1	- Reunião "Kick-off" - Levantamento de requisitos e ativos. - Levantamento do ambiente e projeto para implantação do SIEM.	15 dias após a assinatura do contrato
ETAPA 2	- Implantação do SIEM - Configuração dos ativos.	30 dias após a ETAPA 1
ETAPA 3	- Disponibilização do Software para acompanhamento do Monitoramento	15 dias após a ETAPA 2

Tabela 4 - Requisitos Temporais Grupo 2

7.2.2. Os prazos de execução detalhados nas Tabelas 3 e 4 são contados a partir da assinatura do contrato, respeitando a sequência das etapas e garantindo o pleno atendimento dos requisitos previstos no Termo de Referência.

7.3. NÍVEIS DE SERVIÇO - Grupo 1 - Firewall (Itens 1 a 6) - (SLA):

7.3.1. Para manutenção do desempenho da Contratada será adotado o **SLA (Service Level Agreement/Acordo de Nível de Serviço)** cujos critérios estão a seguir estabelecidos.

7.3.2. Deve ser considerado o regime de atendimento 8 X 5 em horário comercial das 8:00 às 18:00 horas (horário de Brasília), de segunda à sexta-feira, exceto feriados.

7.3.3. O nível de desempenho no atendimento terá como referência os prazos máximos para resposta aos acionamentos, contados a partir do momento da abertura do chamado, de acordo com os Níveis de Severidade dos Chamados e Tabela de Prazos de Atendimento, conforme quadros abaixo:

NÍVEIS DE SEVERIDADE DOS CHAMADOS

GRAU	DESCRIÇÃO DO EVENTO	TEMPO PARA PRIMEIRO CONTATO APÓS ABERTURA DE CHAMADO	TEMPO DE RESOLUÇÃO DO CHAMADO	VALOR A SER GLOSADO
BAIXO	Serviços disponíveis com ocorrência de falhas ocasionais, consulta sobre problemas, dúvidas gerais. Pequeno impacto. Falha de componentes que não impactam o ambiente da Contratante.	90 minutos	Até 06 (seis) horas	0,2% do valor mensal do contrato por hora de atraso injustificado, até o limite de 10%.
URGENTE	Equipamento parcialmente indisponível ou com diminuição da performance de funcionamento. Falha intermitente que torne o ambiente inoperante. Operação afetada, mas sem interrupção das operações críticas da Contratante.	60 minutos	Até 04 (quatro) horas	0,5% do valor do contrato por hora de atraso injustificado, até o limite de 10%.
CRÍTICO	Equipamento totalmente inoperante, afetando operações críticas da Contratante. Problemas em funcionalidades essenciais.	30 minutos	Até 02 (duas) horas	1% do valor mensal do contrato por hora de atraso injustificado, até o limite de 10 %.

Tabela 5 - Níveis de Severidade dos Chamados - Grupo 1

7.3.4. A Contratada deverá informar o número do chamado e disponibilizar um meio de acompanhamento e evolução até a conclusão.

7.3.5. Entende-se por início do atendimento o primeiro contato, após abertura do chamado, feito pela Contratante para tratar do problema reportado.

7.3.6. Entende-se por término do atendimento a execução do serviço de correção e disponibilização do

equipamento em perfeitas condições de funcionamento no local onde está instalado, tendo sanado todos os problemas relatados pela Contratante na abertura do chamado.

7.3.7. O nível de severidade será informado pela Contratante no momento da abertura de cada chamado.

7.3.8. O nível de severidade poderá ser reclassificado a critério da Contratante.

7.3.9. Nos casos de chamados classificados como Nível de Severidade “CRÍTICO”, o atendimento deverá ser contínuo até a resolução. Os prazos para as demais severidades podem ter sua contagem de tempo interrompida ao final de cada dia útil e reiniciada no primeiro dia útil subsequente.

7.3.10. Caso a solução definitiva requeira um tempo maior que o especificado na “**Tabela 5 - Níveis de Severidade dos Chamados - Grupo 1**”, seja devido à sua complexidade, ou por necessidade de ajustes nas configurações, modificações de software ou substituição do equipamento, uma solução de contorno deve ser sugerida e a severidade adequada à realidade da solução definitiva.

7.3.11. Ao final de cada atendimento, a Contratada deverá emitir relatório técnico contendo as seguintes informações: categoria de prioridade, descrição do problema e da solução, procedimentos realizados, data e hora da abertura e do fechamento do chamado, data e hora do início e término da execução dos serviços, identificação do técnico que realizou o atendimento.

7.3.12. As glosas apuradas em razão da aplicação do **SLA** ocorrerão no faturamento do mês subsequente.

7.3.13. As eventuais glosas no caso de descumprimento do **SLA** não devem ser interpretadas como penalidades, e sim como adequações pelo não atendimento das metas estabelecidas em complemento à mensuração dos serviços efetivamente prestados.

7.3.14. Após a 24ª (vigésima quarta) hora de atraso injustificado para o atendimento e solução do chamado técnico, o Contratante poderá rescindir o contrato, caracterizando-se a inexecução do objeto.

7.4. NÍVEIS DE SERVIÇO - Grupo 2 (Itens 7 e 8) - (SLA)

7.4.1. Para manutenção do desempenho da Contratada será adotado o **SLA (Service Level Agreement/Acordo de Nível de Serviço)** cujos critérios estão a seguir estabelecidos.

7.4.2. Deve ser considerado o regime de atendimento **24 x 7**.

7.4.3. O nível de desempenho no atendimento terá como referência os prazos máximos para resposta aos acionamentos, contados a partir do momento da abertura do chamado, de acordo com a **Tabela 6 - Níveis de Severidade dos Chamados - Grupo 2**, conforme quadro abaixo:

NÍVEIS DE SEVERIDADE DOS CHAMADOS

GRAU	DESCRIÇÃO DO EVENTO	SLA PARA DETECÇÃO	SLA PARA RESPOSTA	SLA PARA SOLUÇÃO	VALOR A SER GLOSADO
BAIXO	Alertas falsos, solicitações de suporte técnico, ou eventos de baixa criticidade	Até 4 (quatro) horas	Até 8 (oito) horas	Até 48(quarenta e oito) horas	0,5% do valor mensal do contrato por hora de atraso injustificado, até o limite de 10%.
URGENTE	Ameaça significativa à operação: de sistemas não críticos, perda de dados não confidenciais, ou degradação do desempenho	Até 2 (duas) horas	Até 04 (quatro) horas	Até 6 (seis) horas	1% do valor mensal do contrato por hora de atraso injustificado, até o limite de 10%.
CRÍTICO	Ameaça imediata a sistemas críticos: perda de dados confidenciais, ou interrupção e serviços essenciais	Até 1 (uma) hora	Até 02 (duas) horas	Até 4 (quatro) horas	2% do valor mensal do contrato por hora de atraso injustificado, até o limite de 10%

Tabela 6 - Níveis de Severidade dos Chamados - Grupo 2

7.4.4. O SLA da disponibilidade do serviço terá como referência as metas definidas na tabela abaixo:

Indicador	Meta	Base para Penalidade	Penalidade
Disponibilidade do suporte técnico	24x7	Indisponibilidade do suporte	1% do valor mensal do contrato por hora de indisponibilidade
Relatório de incidente de segurança	Até 05 dias úteis após a conclusão do incidente	Atraso na entrega	0,5% do valor mensal do contrato por dia de atraso
Disponibilidade do serviço	24x7	Tempo de indisponibilidade	1% do valor mensal do contrato por hora de indisponibilidade
Conclusão do monitoramento de ativos	Até 90 (noventa) dias do início da execução do contrato	Atraso na implantação do monitoramento	0,5% do valor mensal do contrato por dia de atraso

Tabela 7 - Disponibilidade do Serviço

7.4.5. A Contratada deverá informar o número do chamado e disponibilizar um meio de acompanhamento e evolução até a conclusão.

7.4.6. Entende-se por início do atendimento o primeiro contato, após abertura do chamado, feito pela Contratante para tratar do problema reportado.

7.4.7. Entende-se por término do atendimento a execução do serviço de correção, tendo sanado todos os problemas relatados pela Contratante na abertura do chamado.

7.4.8. O nível de severidade será informado pela Contratante no momento da abertura de cada chamado.

7.4.9. O nível de severidade poderá ser reclassificado a critério da Contratante.

7.4.10. Nos casos de chamados classificados como Nível de Severidade “CRÍTICO”, o atendimento deverá ser contínuo até a resolução. Os prazos para as demais severidades podem ter sua contagem de tempo interrompida ao final de cada dia útil e reiniciada no primeiro dia útil subsequente.

7.4.11. Caso a solução definitiva requeira um tempo maior que o especificado na “**Tabela 6- Níveis de Severidade dos Chamados - Grupo 2**”, seja devido à sua complexidade, ou por necessidade de ajustes nas configurações, modificações de software ou substituição do equipamento, uma solução de contorno deve ser sugerida e a severidade adequada à realidade da solução definitiva.

7.4.12. Ao final de cada atendimento, a Contratada deverá emitir relatório técnico contendo as seguintes informações: categoria de prioridade, descrição do problema e da solução, procedimentos realizados, data e hora da abertura e do fechamento do chamado, data e hora do início e término da execução dos serviços, identificação do técnico que realizou o atendimento.

7.4.13. As glosas apuradas em razão da aplicação do **SLA** ocorrerão no faturamento do mês subsequente.

7.4.14. As eventuais glosas no caso de descumprimento do **SLA** não devem ser interpretadas como penalidades, e sim como adequações pelo não atendimento das metas estabelecidas em complemento à mensuração dos serviços efetivamente prestados.

7.4.15. Após a 24ª (vigésima quarta) hora de atraso injustificado para o atendimento e solução do chamado técnico, o Contratante poderá rescindir o contrato, caracterizando-se a inexecução do objeto.

7.4.16. O monitoramento e a apuração dos **SLAs** serão realizados com base nos dados extraídos das ferramentas e plataformas utilizadas pela CONTRATADA, as quais deverão estar disponíveis ao TRIBUNAL DE CONTAS DE RORAIMA para fins de validação, fiscalização e auditoria.

7.5. Requisitos de Suporte Técnico, Manutenção e Garantia.

7.5.1. Suporte Técnico:

7.5.1.1. O serviço de suporte técnico à solução destina-se:

- a) A Instalação, configuração, correção de problemas e esclarecimento de dúvidas sobre configuração e

utilização da solução ofertada;

b) A empresa deve possuir no momento da assinatura do contrato, pelo menos 1 (um) profissional com certificação técnica emitida pelo fabricante, capaz de prestar o Serviço Especializado;

c) A CONTRATADA é responsável pelo gerenciamento dos chamados e fornecimento de informações à CONTRATANTE, mesmo que haja escalonamento ao fabricante.

7.5.2. Manutenção dos Equipamentos (Grupo 1):

7.5.2.1. A contratada deverá prestar o serviço de manutenção dos equipamentos do Grupo 1 (Itens 1 e 2) durante a vigência do contrato.

7.5.2.2. Os equipamentos deverão possuir garantia do fabricante de **60 (sessenta) meses** para entrega de peças *on-site* em Boa Vista/RR.

7.5.2.3. O(s) fabricante(s) deverá(ão) emitir os Termos de Garantia dos equipamentos a serem fornecidos pela Contratada.

7.5.2.4. A empresa a ser Contratada poderá substituir o equipamento danificado por outro novo com especificações similares ou superiores, a seu critério, desde que tal substituição seja aprovada pela equipe técnica do TCERR e não represente qualquer tipo de prejuízo ao erário.

7.5.2.5. Manutenção corretiva: Entende-se por manutenção corretiva a série de procedimentos destinados a recolocar os equipamentos em seu perfeito estado de uso, compreendendo, inclusive, substituições de peças, ajustes e reparos necessários, de acordo com os manuais e normas técnicas específicas para os equipamentos.

7.5.2.6. Na ocorrência de manutenção corretiva, os componentes substituídos deverão ser novos, sem utilização anterior, com configuração igual ou superior aos originais e em linha de produção. Caso o componente não se encontre mais disponível no mercado, deve-se observar que o componente substituído deve ter, no mínimo, a mesma qualidade e especificações técnicas do componente fora de linha.

7.5.2.7. Sendo constatada a necessidade de substituição do equipamento pela equipe de suporte técnico da Contratada, o procedimento será efetuado sem qualquer ônus para a Contratante.

7.5.2.8. Manutenção preventiva: Entende-se por manutenção preventiva aquela que é realizada periodicamente para evitar paradas e manter o equipamento em condições de trabalho normal, programada em comum acordo com a Contratante, de modo a evitar ao máximo a indisponibilidade dos equipamentos contratados.

7.5.2.9. Na realização da manutenção preventiva a Contratada deverá realizar revisões, testes e adequações nos equipamentos visando a garantir o melhor desempenho da solução contratada.

7.5.2.10. Serão executadas, no mínimo, **2 manutenções preventivas** a cada período de **12 meses** de contrato, sem ônus adicional à Contratante.

7.5.2.11. Caso, para a solução do problema, seja necessária a retirada do equipamento das dependências do prédio sede desta Corte, a Contratada poderá fazê-lo exclusivamente às suas expensas, mantendo inalterado o prazo para conclusão do trabalho.

7.5.2.12. Na hipótese de produto que necessite de peças ou partes importadas e não comuns de mercado, a critério da fiscalização do contrato, o prazo para a conclusão dos trabalhos poderá ser ampliado.

7.5.3. Requisitos de Negócio:

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

7.5.3.1.1 Garantir que a infraestrutura da rede de dados do TCERR seja monitorada e melhorada, permitindo melhor defesa a ataques cibernéticos;

7.5.3.1.2. Garantir a disponibilidade, continuidade e qualidade dos serviços para o cumprimento das atividades finalísticas do Tribunal e, conseqüentemente, o alcance dos resultados desejados para a sociedade;

7.5.3.1.3. Garantir os meios adequados para que os processos de segurança da informação possam ser aprimorados através da implementação de recursos de proteção adequados.

7.5.4. Requisitos de Capacitação - Grupo 1

7.5.4.1. O treinamento à equipe local do Tribunal será realizado na modalidade presencial, preferencialmente nos períodos das 08:00 às 12:00 e das 14:00 às 18:00, em dias úteis e em horário a ser definido pelo Tribunal;

7.5.4.2. O treinamento deverá ter uma **carga horária mínima de 16 horas**;

7.5.4.3. A contratada deverá ministrar treinamento para até 5 participantes da equipe técnica da Contratante;

7.5.4.4. O treinamento deverá abranger o repasse de informações e conhecimentos referentes à administração e gerenciamento da solução Itens (1,2 e 3), bem como o esclarecimento de dúvidas.

7.5.4.5. O treinamento deverá ser ministrado em língua portuguesa por profissional certificado pelo fabricante do produto ofertado.

8. PARCELAMENTO DO OBJETO

O objeto do presente Termo será parcelado em dois grupos – **Grupo 1: Firewall** e **Grupo 2: SOC** – em razão da natureza distinta dos serviços, da possibilidade de execução independente de cada grupo e da necessidade de ampliar a competitividade do certame, em conformidade com o disposto no [art. 40, inciso V, alínea "b", da Lei nº 14.133/2021](#).

9. CRITÉRIOS DE SUSTENTABILIDADE

Não se aplica.

10. PRAZO E LOCAL DE ENTREGA

10.1. O prazo para início da execução contratual será a partir da assinatura do contrato, devendo, a partir desse momento, seguir o cronograma detalhado de execução das etapas, conforme **item 7 – Forma de Execução**.

10.2. Os prazos específicos de entrega, instalação, implantação e treinamento seguirão as etapas e prazos estabelecidos nas Tabelas 3 e 4 do item 7 deste Termo.

10.3. O local de entrega, instalação e execução dos serviços relacionados ao **Grupo 1** será nas dependências do Tribunal de Contas do Estado de Roraima (TCERR), ou em outro local que venha a ser formalmente indicado pela Contratante.

10.4. O prazo de entrega do objeto poderá ser prorrogado de forma excepcional, mediante justificativa fundamentada e aprovação da fiscalização do contrato, observando os limites previstos na Lei nº 14.133/2021.

11. GARANTIA E ASSISTÊNCIA TÉCNICA

Os requisitos de garantia e assistência técnica estão detalhados no *item 7.5. Requisitos de Suporte Técnico, Manutenção e Garantia*.

12. VIGÊNCIA DO CONTRATO

12.1. O prazo de vigência do contrato será contado a partir da assinatura, podendo ser prorrogado nos termos do art. 107 da Lei nº 14.133/2021, com as seguintes especificações:

12.1.1. **Grupo 1 – Firewall:** vigência de **60 meses** para fornecimento, manutenção e suporte dos equipamentos e softwares relacionados.

12.1.2. **Grupo 2 – SOC:** vigência de **36 meses** para prestação de serviços de monitoramento, suporte e atendimento remoto.

12.2. A gestão contratual, eventuais prorrogações, fiscalizações e encerramentos de cada grupo serão conduzidos de forma **autônoma**, observando-se seus respectivos prazos e condições específicas.

12.3. Havendo interesse, a vigência do contrato poderá ser prorrogada condicionada a:

12.3.1. Preços e condições vantajosas;

12.3.2. Regularidade fiscal e trabalhista;

12.3.3. Inexistência de sanção impeditiva, comprovada por meio da consulta no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e Cadastro Nacional de Empresas Punidas (CNEP), podendo ser substituídas pela Consulta Consolidada no portal do Tribunal de Contas da União (TCU).

12.4. A vigência contratual de cada grupo de serviços terá início a partir da data da última assinatura das partes no termo de contrato, sendo a contagem do prazo **independente para cada grupo**, conforme seus respectivos cronogramas e especificações.

13. **MODELO DE GESTÃO DO CONTRATO**

13.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas contidas na Lei nº 14.133/2021, onde cada parte responderá pelas consequências do seu descumprimento, seja parcial ou total.

13.2. A execução do contrato será acompanhada e fiscalizada por fiscal ou equipe de fiscalização devidamente designada para esse fim, com atribuições de representar administrativamente o Contratante e proceder o recebimento do objeto quando não designada comissão de recebimento.

13.3. As competências e atribuições do fiscal e da equipe de fiscalização estão regulamentadas por meio da **Resolução nº 20/2023/TCERR-PLENO**, ep. 0843916.

13.4. O Contratado deverá informar imediatamente à fiscalização fato que impeça o cumprimento tempestivo da entrega ou execução do objeto.

13.5. Nos contratos por escopo, o Contratado deverá manter o Contratante sempre informado acerca do andamento da entrega do objeto, devendo disponibilizar, sempre que possível, os dados de rastreio para acompanhamento.

13.6. As comunicações entre o Contratante e o Contratado que exigirem formalidade de atos deverão ser realizadas sempre por meio eletrônico.

13.7. Identificada qualquer inexistência ou irregularidade no cumprimento das cláusulas contratuais, o responsável pela fiscalização emitirá notificações para a correção, determinando prazo adequado para tal ato.

13.8. Caso ocorram descumprimento das obrigações contratuais, o responsável pela fiscalização atuará tempestivamente na solução do problema, reportando os fatos ao gestor de contratos para que tome as providências cabíveis, quando ultrapassar a sua competência.

13.9. Havendo injustificado inadimplemento contratual, o responsável pela fiscalização autuará processo administrativo específico para a apuração da conduta faltosa do Contratado, observando as diretrizes contidas na **Resolução nº 002/2024-TCERR-PLENO**, ep. 1034993.

14. **FORMA E CONDIÇÕES DE RECEBIMENTO**

14.1. O objeto contratual será recebido pelo fiscal do contrato ou pela equipe designada, conforme as etapas previstas para o **Grupo 1 (Firewall)** e o **Grupo 2 (SOC)**, observando os prazos estabelecidos nas respectivas tabelas de requisitos temporais (itens 7.1.1. e 7.1.2.)

14.1.1 Recebimento Provisório

14.1.1.1 Grupo 1 – Firewall: ocorrerá após a conclusão da ETAPA 2 conforme cronograma da Tabela 3, ou seja, 50 (cinquenta) dias após a assinatura do contrato.

14.1.1.2 Grupo 2 – SOC: ocorrerá após a conclusão da ETAPA 2 conforme cronograma da Tabela 4, ou seja, 45 (quarenta e cinco) dias após a assinatura do contrato.

14.1.2 Recebimento Definitivo

14.1.2.1 Grupo 1 – Firewall: até 10 (dias) úteis após a conclusão da ETAPA 3 conforme cronograma da Tabela 3.

14.1.2.2 Grupo 2 – SOC: até 10 (dias) úteis após a conclusão da ETAPA 3 conforme cronograma da Tabela 4.

14.2. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, desde que justificado junto ao fiscal do contrato.

14.3. Os bens entregues poderão ser rejeitados no todo ou em parte, inclusive antes do recebimento provisório, quando estiverem em desacordo com as especificações constantes no Termo de Referência e proposta adjudicada, devendo ser substituídos às custas do Contratado no prazo de até **10 dias úteis**, a contar da notificação, sem prejuízo da aplicação das penalidades cabíveis.

14.4. O prazo para o saneamento de inconsistências na execução do objeto não será computado para os fins de recebimento definitivo.

14.5. O recebimento provisório ou definitivo não exclui a responsabilidade pelas obrigações contratuais posteriores e garantia pertinente ao objeto.

14.6. Por se tratar de serviço continuado, executado por demanda e com pagamento mensal, a liquidação deverá, ao final de cada mês, ser instruída minimamente com: 1) Nota Fiscal; 2) Atesto; 3) Relatório de Acompanhamento; e 4) Despacho de Liquidação e Pagamento, dirigido à Unidade competente.

15. FORMA E CONDIÇÕES DE PAGAMENTO

15.1. Condições de Pagamento por Grupo e Natureza do Serviço:

15.1.1. **Grupo 1 (FIREWALL) - Serviços Contínuos (Itens 1, 2 e 3):** O pagamento será efetuado mensalmente, durante 60 meses, ao final de cada período de execução dos serviços contínuos, mediante a conclusão e aceite dos serviços prestados, conforme critérios estabelecidos no Item 14 (Forma e Condições de Recebimento).

15.1.2. **Grupo 1 (FIREWALL) - Serviços de Implantação e Treinamento (Itens 4 e 5):** O pagamento referente aos serviços de Implantação, Migração e Configuração (Item 4) e Treinamento da equipe técnica (Item 5) será realizado após a conclusão e aceite da ETAPA 4 (Treinamento), conforme cronograma estabelecido na Tabela 3.

15.1.3. **Grupo 1 (FIREWALL) - Serviços Sob Demanda (Item 6):** O pagamento pelos Serviços Técnicos Especializados em Segurança da Informação (Item 6) será efetuado por demanda, mediante a emissão prévia de Ordens de Serviço (OS) e após a entrega dos serviços com respectivo relatório de execução, referente a 120 UST distribuídas ao longo do período de 60 meses.

15.1.4. **Grupo 2 (SOC) - Serviços Contínuos (Item 7):** O pagamento será efetuado mensalmente, durante 36 meses, ao final de cada período de execução dos serviços contínuos, mediante a conclusão e aceite dos serviços prestados, conforme critérios do Item 14.

15.1.5. **Grupo 2 (SOC) - Serviços Sob Demanda (Item 8):** O pagamento pelos Serviços Técnicos Especializados (SOC) sob demanda será realizado mediante a emissão prévia de Ordens de Serviço (OS) e entrega dos serviços com respectivo relatório de execução, referente a 1.080 UST distribuídas ao longo de 36 meses.

15.2. Para fins de pagamento, a nota fiscal eletrônica será encaminhada pelo Contratado, via *e-mail*, exclusivamente ao fiscal do contrato, cujo endereço eletrônico será repassado oportunamente.

15.3. Orientações para a emissão da nota fiscal ou documento equivalente para fins de retenção tributária:

15.3.1. O Contratado deverá observar quando da emissão da nota fiscal ou documento de cobrança equivalente às disposições da **Instrução Normativa RFB nº 1234/2012** alterada pela **Instrução Normativa RFB nº 2145/2023**, em especial o **art. 2º-A, parágrafos 2º e 3º** e os **arts. 3º e 11**, e os **anexos da instrução normativa** inicialmente citada, sem prejuízos do cumprimento das legislações pertinente ao INSS (União), ICMS (Estado) e ISS (Município);

15.3.2. As alíquotas dos tributos decorrentes da atividade empresarial do Contratado deverão constar expressamente no corpo da nota fiscal ou documento equivalente, bem como as informações acerca de eventual isenção tributária;

15.3.3. Em razão da extinção do convênio entre o Governo do Estado de Roraima e a União (DOU 219 de 22/11/2022 - Seção 3/Pag. 50), passam a ser de exclusiva responsabilidade do Contratado o recolhimento da **CSLL, COFINS e PIS/PASEP**.

15.4. Caso o Contratado não cumpra integralmente o disposto no item anterior, o pagamento não será processado até que ocorra a devida correção.

15.5. O Contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123/2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime, desde que apresente comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida lei complementar.

15.6. O pagamento ocorrerá em **até 10 dias úteis**, após o atesto da nota fiscal, por meio de ordem bancária para crédito no banco, agência e conta corrente indicados pelo Contratado.

15.7. Para fins de pagamento, o Contratado deverá estar adimplente com a Fazenda Federal e Estadual e/ou Municipal, incluindo a regularidade perante a Justiça do Trabalho e ao Fundo de Garantia por Tempo de Serviço (FGTS).

15.8. Não será aceito como comprovação da regularidade fiscal perante a Fazenda Municipal a certidão emitida/validada na condição de contribuinte.

15.9. A nota fiscal que for apresentada com erro deverá ser imediatamente substituída, ficando o pagamento suspenso e o prazo para pagamento suspenso até que o Contratado providencie a substituição.

15.10. No preço contratado deverão estar inclusos todos os tributos, taxas, encargos, seguros, fretes e quaisquer outras despesas que incidam sobre o objeto.

15.11. No caso de atraso do pagamento, salvo se por culpa do Contratado, serão devidos pelo Contratante encargos moratórios à taxa nominal de 6% a.a. (seis por cento ao ano), capitalizados diariamente em regime de juros simples, conforme a seguinte fórmula: $EM = I \times N \times VP$, onde: EM = Encargos moratórios devidos. N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento. I = Índice de compensação financeira = 0,00016438. e VP = Valor do pagamento em atraso.

16. MATRIZ DE RISCO

Não se aplica.

17. FORMA E CONDIÇÕES DE REAJUSTAMENTO

17.1. Os preços contratados poderão ser reajustados após 12 (doze) meses, contados da data do orçamento estimado de **23/10/2025**, com base na variação do **Índice de Custo da Tecnologia da Informação – ICTI**, divulgado pelo IPEA, ou de outro índice que venha a substituí-lo oficialmente, em conformidade com o [art. 92, §3º, da Lei nº 14.133/2021](#).

17.2. Para o cálculo do índice de reajustamento será adotada a seguinte **fórmula**:

$$IR = (if - ii) / ii$$

Onde:

IR = Índice de Reajustamento.

ii - índice inicial: índice do mês de apresentação da proposta.

if - índice final: índice correspondente a data do reajuste.

17.3. O reajuste de preços deverá ser solicitado formalmente pelo Contratado antes de eventual prorrogação do contrato, decaindo tal direito caso seja firmado termo aditivo prorrogatório sem a devida manifestação quanto ao reajuste.

17.4. Revisão de Preços:

17.4.1. A revisão dos preços contratados poderá ocorrer a qualquer tempo, com a finalidade de garantir a manutenção do equilíbrio econômico do contrato, podendo ocorrer da seguinte forma:

a) Pelo Contratante, nos casos em que for verificada a redução do preço praticado no mercado ou em decorrência de redução de carga tributária ou de estudos técnicos elaborados internamente;

b) Pelo Contratado, mediante solicitação formal e fundamentada e acompanhada da planilha de composição de custo do novo preço, contendo os mesmos elementos formadores dos preços contratados, devendo demonstrar quais os itens da planilha de custos estão defasados e que estão ocasionando o desequilíbrio do contrato.

17.4.2. Em nenhuma hipótese os preços revisados ultrapassarão os praticados no mercado.

17.4.3. Caso a revisão seja concedida, ocorrerá a partir da data da assinatura do respectivo termo aditivo, com efeitos financeiros a partir da data da solicitação do Contratado.

18. OBRIGAÇÕES DO CONTRATADO

18.1. Providenciar, imediatamente após o recebimento da nota de empenho, as tratativas necessárias ao cumprimento célere do encargo disposto neste Termo.

18.2. Prestar os serviços no prazo pactuado, sob pena de aplicação das penalidades previstas neste Termo.

18.3. Prestar a garantia necessária dos serviços conforme solicitado neste Termo de Referência.

18.4. Disponibilizar pessoal qualificado e habilitado para a execução dos serviços, conforme indicado no item 7.5.1.1.b e 24.4 do presente instrumento;

18.5. A CONTRATADA obriga-se a manter a estabilidade da equipe técnica envolvida nos projetos, providenciando a substituição de colaboradores que eventualmente se desliguem da equipe, garantindo o padrão técnico e a qualidade dos trabalhos.

18.6. Decidir em comum acordo com a CONTRATANTE sobre os métodos, detalhes e meios através dos quais os serviços serão executados, utilizando pessoal com qualificação técnica necessária e em número suficiente para atender a demanda;

18.7. Fornecer à CONTRATANTE, sempre que formalmente solicitado, informações detalhadas sobre o andamento dos serviços;

18.8. Reparar, corrigir ou substituir, às suas expensas, no total ou em parte, os serviços em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados;

18.9. Responder, integralmente, por perdas e danos que vier a causar ao contratante ou à terceiros em razão de ação ou omissão, dolosa ou culposa, de seus empregados, independente de outras cominações contratuais ou legais a que estiver sujeita;

18.10. Entregar, ao final de períodos estabelecidos em comum acordo pelas partes, toda a documentação oriunda da execução das atividades relacionadas ao presente contrato.

18.11. A CONTRATADA obriga-se a manter a confidencialidade das informações compartilhadas e que não sejam de domínio público, além daqueles referentes ao conteúdo e tecnologia envolvida no projeto, exceto quando autorizado por escrito pela CONTRATANTE.

18.12. Manter durante toda a execução do contrato as condições de habilitação e qualificação exigidas no procedimento licitatório, devendo comunicar ao Contratante a superveniência de fato impeditivo da manutenção dessas condições.

18.13. Não subcontratar o objeto do presente Termo.

19. OBRIGAÇÕES DO CONTRATANTE

19.1. Efetuar o pagamento no prazo informado neste termo.

19.2. Acompanhar e fiscalizar a execução do contrato por meio de servidor designado para esse fim.

19.3. Verificar o cumprimento das especificações exigidas, podendo rejeitá-las quando não atenderem este termo.

19.4. Prestar informações necessárias ao Contratado para a perfeita execução do contrato.

20. GARANTIA CONTRATUAL

20.1. Com a finalidade de assegurar a execução do contrato e suprir eventual situação de inadimplência, o Contratado apresentará **garantia contratual** na forma do art. 96 da Lei nº 14.133/2021, em até **30 dias**, após a homologação do certame e antes da assinatura do contrato, no percentual de **5%** do valor da contratação, podendo optar por uma das **modalidades de garantia** abaixo:

20.1.1. **Caução em Dinheiro:** a garantia em dinheiro deverá ser efetuada, obrigatoriamente, em conta específica, em favor do Contratante;

20.1.2. **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;

20.1.3. **Seguro Garantia:** será realizado mediante a entrega da apólice, inclusive digital, emitida por empresa em funcionamento no Brasil e devidamente registrada na Superintendência de Seguros Privados - SUSEP, sendo a Contratante o único beneficiário/segurado, observando-se, ainda, as disposições do art. 97 da Lei nº 14.133/2021;

20.1.4. **Fiança Bancária:** mediante entrega de carta de fiança fornecida por estabelecimento bancário, devidamente registrada em cartório de registro de títulos e documentos, conforme determinado no art. 129 da Lei nº 6.015/73. Na Fiança Bancária, deverá constar do instrumento a expressa renúncia pelo fiador dos benefícios previstos nos artigos 827 e 835 do Código Civil Brasileiro;

20.1.5. **Título de capitalização** custeado por pagamento único, com resgate pelo valor total.

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

- 20.2.1. Prejuízos advindos do não cumprimento do contrato e do não adimplemento das demais obrigações nele previstas;
 - 20.2.2. Prejuízos causados à Administração ou a terceiro, decorrentes de culpa ou dolo durante a execução do contrato;
 - 20.2.3. Multas moratórias e punitivas aplicadas pelo Contratante; e
 - 20.2.4. Obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza não adimplidas pelo Contratado, conforme a natureza do contrato.
- 20.3. Os dados do contrato garantido e/ou assegurado deverão constar no instrumento de garantia ou seguro a ser apresentado pelo garantidor e/ou segurador.
- 20.4. A garantia contratual terá validade mínima de **90 dias** além da vigência contratual, devendo ser renovada e atualizada no caso de alteração do valor e/ou prorrogação do contrato.
- 20.5. A garantia contratual será liberada ou restituída somente após a comprovação de que o Contratado cumpriu as obrigações contratuais.

21. SANÇÕES ADMINISTRATIVAS

21.1 Comete infração administrativa no âmbito da execução do contrato, nos termos da Lei nº 14.133/2021, o Contratado que:

- 21.1.1. dar causa à inexecução parcial do contrato;
- 21.1.2. dar causa à inexecução parcial do contrato, que cause grave dano ao Contratante;
- 21.1.3. dar causa à inexecução total do contrato;
- 21.1.4. ensejar o retardamento da execução ou da entrega do objeto sem motivo justificado;
- 21.1.5. prestar declaração falsa durante a execução do contrato;
- 21.1.6. praticar ato fraudulento na execução do contrato;
- 21.1.7. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- 21.1.8. praticar ato lesivo previsto no art. 5º da Lei nº 12.846/2013.

21.2. O Contratado que cometer quaisquer das infrações discriminadas no item 21.1 ficará sujeito, sem prejuízo das responsabilidades civil e criminal, às seguintes sanções:

- 21.2.1 **ADVERTÊNCIA:** no caso de cometimento da infração administrativa prevista no subitem 21.1.1, quando **não se justificar** a imposição de penalidade mais grave.
- 21.2.2. **MULTA:**
 - a) de **10%** sobre o valor do contrato no caso de cometimento das infrações administrativas previstas nos subitens 21.1.1 e 21.1.4;
 - b) de **15%** sobre o valor do contrato no caso de cometimento das infrações administrativas previstas nos subitens 21.1.2 e 21.1.3;
 - c) de **20%** sobre o valor do contrato no caso de cometimento das infrações administrativas previstas nos subitens 21.1.5 a 21.1.8.
- 21.2.3. **MULTA MORATÓRIA :** de **0,5%** sobre o valor do contrato ou item, **por dia de atraso injustificado** na execução do objeto, limitada a **30%** , podendo ser convertida em **multa compensatória** no caso de extinção unilateral do contrato, sem prejuízo da aplicação cumulativa com outras sanções previstas em lei.
 - 21.2.3.1. Não havendo **garantia contratual**, ocorrerá a **retenção preventiva** do valor presumido da **multa moratória** antes da instauração do regular procedimento administrativo;
 - 21.2.3.2. Se a **multa** aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada, se houver, ou será cobrada judicialmente.
- 21.2.4. **IMPEDIMENTO DE LICITAR E CONTRATAR:** pelo prazo de **2 anos**, no caso de cometimento das infrações administrativas previstas nos subitens 21.1.2 e 21.1.3, e de **6 meses**, no caso de cometimento da infração administrativa previstas no subitem 21.1.4, quando **não se justificar** a imposição de penalidade mais

grave.

21.2.5. **DECLARAÇÃO DE INIDONEIDADE:** pelo prazo de **3 anos**, no caso de cometimento das infrações administrativas previstas nos **subitens 21.1.5 e 21.1.6**, e de **6 anos**, no caso de cometimento da infração administrativa previstas no **subitens 21.1.7 e 21.1.8**, bem como pelo prazo de **3 anos**, no caso de cometimento das infrações **21.1.2 a 21.1.4**, quando **se justificar** a imposição de penalidade mais grave.

21.2.6. As sanções previstas nos **subitens 21.2.1, 21.2.4 e 21.2.5** poderão ser aplicadas **cumulativamente** com a prevista no **subitem 21.2.2**.

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

21.4. O exercício do direito ao **contraditório** e a **ampla defesa** acerca da imputação das infrações previstas neste item ocorrerá no âmbito do **processo administrativo sancionatório**.

21.5. O **processo administrativo sancionatório** seguirá às disposições da **Resolução nº 02/2024-TCERR-PLENO**.

21.6. No caso de abertura de **processo administrativo sancionatório** destinado a apuração de infrações contratuais e eventual aplicação de sanção administrativa, as comunicações ao Contratado serão realizadas preferencialmente por meio do endereço de correio eletrônico (e-mail) informado na proposta adjudicada ou o constante no Sistema de Cadastro Unificado de Fornecedores (SICAF).

21.6.1. O Contratado deverá manter atualizado o endereço de correio eletrônico (e-mail) informado na proposta e no Sistema de Cadastro Unificado de Fornecedores (SICAF), e confirmar o recebimento das mensagens provenientes do Tribunal de Contas do Estado de Roraima, não podendo alegar o desconhecimento do recebimento das comunicações por este meio como justificativa para se eximir das responsabilidades assumidas ou de eventuais sanções aplicadas.

22. CONDIÇÕES DE PARTICIPAÇÃO NO PROCEDIMENTO DE CONTRATAÇÃO

22.1. Em razão das vedações legais, não poderá participar do procedimento de contratação:

22.1.1. A empresa ou empresário impedido licitar e contratar com órgãos e entidades estaduais e municipais no Estado de Roraima, durante o prazo da sanção aplicada.

22.1.2. O empresário declarado inidôneo perante a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação.

22.1.3. Aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do Contratante ou com servidor que desempenhe função no procedimento licitatório ou na contratação direta, bem como 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.

22.1.4. O empresário cujo instrumento constitutivo não seja compatível com o objeto deste termo.

22.1.5. Sociedade estrangeira não autorizada a funcionar no Brasil.

22.1.6. As sociedades integrantes de um mesmo grupo econômico, assim entendidas aquelas que tenham diretores, sócios ou representantes legais comuns, ou que utilizem recursos materiais, tecnológicos ou humanos em comum, exceto se demonstrado que não agem representando interesse econômico em comum.

22.1.7. Aquele que se enquadrar nas demais vedações previstas no art. 14 da Lei nº 14.133/2021.

22.2. O atendimento das condições indicadas nos **subitens 22.1.1 e 22.1.2** serão supridas por meio de **Consulta Consolidada** no portal do **Tribunal de Contas da União (TCU)** ou SICAF ou por qualquer outro meio idôneo de consulta.

23. FORMA E CRITÉRIO DE SELEÇÃO

23.1. A seleção do fornecedor ocorrerá por meio de **procedimento licitatório** na modalidade **Pregão**, sob a forma **Eletrônica**, com adoção do **critério de julgamento** pelo **menor preço**, conforme **Resolução nº 21/2023 - TCERR - PLENO**, ep. 0823180.

23.2. A proponente/licitante que não mantiver a proposta quando vencedora ou quando convocada no prazo da validade da sua proposta, poderá sofrer as sanções administrativas previstas na **Resolução nº 02/2024-TCERR-PLENO**, ep. 1034993, assegurados o contraditório e a ampla defesa.

23.3. É dever da proponente/licitante avaliar previamente se tem condições financeiras e operacionais para participar do certame e se vencedora, cumprir o objeto do contrato nas condições e prazos indicados neste termo, sob pena das sanções administrativas previstas na resolução indicada no item anterior.

24. EXIGÊNCIAS DE HABILITAÇÃO

Sem prejuízo dos demais documentos que venham a ser solicitados em edital de licitação, a licitante deverá apresentar os documentos abaixo para fins de habilitação:

24.1. Habilitação Jurídica:

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

24.1.2. **Sociedade Empresária, Sociedade Limitada Unipessoal – SLU** ou sociedade identificada como **Empresa Individual de Responsabilidade Limitada - EIRELI:** inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

24.1.3. **Sociedade Empresária Estrangeira:** portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede;

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

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

24.1.6. **Consórcio:** Não será permitida a participação de pessoa jurídica constituída por meio de consórcio, em razão do baixo valor e da baixa complexidade do objeto, sob pena de perder a economia de escala.

24.2. Habilitação Fiscal, Social e Trabalhista:

24.2.1. Prova de inscrição no **Cadastro Nacional de Pessoas Jurídicas;**

24.2.2. Prova de regularidade fiscal perante a **Fazenda Nacional**, mediante apresentação de **certidão conjunta federal** expedida pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional;

24.2.3. Prova de regularidade junto ao **Fundo de Garantia do Tempo de Serviço (FGTS);**

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

24.2.5. Prova de inscrição no **cadastro de contribuintes municipal** relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual.

24.2.6. Prova de regularidade com a **Fazenda Municipal** do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre.

24.2.7. **Declaração de Inexistência de Trabalho Infantil**, em cumprimento do inciso XXXIII, da Constituição Federal.

24.2.8. Em se tratando de **filial**, os documentos de **habilitação jurídica e regularidade fiscal** deverão estar em nome da filial, exceto aqueles que, pela própria natureza, são emitidos somente em nome da matriz

24.2.9. Caso a licitante seja considerada isenta dos tributos estaduais ou municipais relacionados ao objeto da contratação, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda Estadual ou Municipal do seu domicílio ou sede, ou outra equivalente, na forma da lei.

24.3. Qualificação Econômico-Financeira:

24.3.1. Certidão Negativa de Falência expedida pelo distribuidor da sede do fornecedor.

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

a) *Liquidez Geral (LG) = (Ativo Circulante + Realizável a Longo Prazo) / (Passivo Circulante + Passivo Não Circulante);*

b) *Solvência Geral (SG) = (Ativo Total) / (Passivo Circulante + Passivo não Circulante); e*

c) *Liquidez Corrente (LC) = (Ativo Circulante) / (Passivo Circulante).*

24.3.3. Empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências de habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura, nos termos do art. 65, §1º, da Lei nº 14.133/2021.

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

24.3.5. Os documentos acima referenciados deverão ser exigidos com base no limite definido pela **Receita Federal do Brasil** para transmissão da **Escrituração Contábil Digital - ECD** ao **SPED**.

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

24.4. Qualificação Técnica:

24.4.1. A licitante deverá apresentar Atestado de Capacidade Técnica ou documento equivalente, emitido por pessoa jurídica de direito público ou privado, comprovando a execução de serviços compatíveis com o objeto deste Termo de Referência.

24.4.2. A licitante deverá disponibilizar, quando solicitado pelo TCERR, informações que permitam comprovar a legitimidade dos atestados apresentados, incluindo, mas não se limitando a: cópia do contrato que deu origem à prestação dos serviços, endereço da contratante, local de execução do objeto e outros documentos julgados necessários para atestar a idoneidade do(s) atestado(s).

24.4.3. A habilitação da licitante poderá ser comprovada por meio do Sistema de Cadastro Unificado de Fornecedores (SICAF), nos documentos por ele abrangidos.

25. REQUISITOS DA CONTRATAÇÃO

25.1. Para garantir a conformidade com as melhores práticas internacionais de privacidade e segurança da informação, a contratada deverá possuir, no mínimo, as seguintes certificações:

25.1.1. **Grupo 1 (FIREWALL):** O profissional responsável pelo suporte técnico deverá possuir certificação CISSP (Certified Information Systems Security Professional) ou equivalente.

25.1.2. **Grupo 2 (SOC):** A contratada deverá possuir a certificação ISO/IEC 27001 e, em seu corpo de funcionários, as seguintes certificações:

25.1.2.1. CEH (Certified Ethical Hacker), emitida pelo EC-Council ou equivalente;

25.1.2.2. CISSP (Certified Information Systems Security Professional) ou equivalente;

25.1.2.3. ECSA (Certified Security Analyst), emitida pelo EC-Council ou equivalente;

25.1.2.4. GCIH (GIAC Certified Incident Handler), emitida pelo GIAC ou equivalente;

25.1.2.5. GCIA (GIAC Certified Intrusion Analyst), emitida pelo GIAC ou equivalente.

25.2. Todas as certificações devem estar válidas durante a execução do contrato, com comprovação oficial pelos organismos certificadores reconhecidos, constituindo **requisito obrigatório apenas** para a **assinatura do contrato**, não sendo exigidas na **fase de habilitação**.

26. PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

26.1. As partes se comprometem a proteger os direitos fundamentais de liberdade e de privacidade e o livre

desenvolvimento da personalidade da pessoa natural, relativos ao tratamento de dados pessoais, nos termos da Lei Geral de Proteção de Dados - LGPD (Lei nº 13.709/2018).

26.2. O Contratado obriga-se ao dever de proteção, confidencialidade, sigilo da informação, dados pessoais e base de dados a que tiver acesso, nos termos da LGPD em razão da execução do contrato.

26.3. O Contratado não poderá utilizar informações, dados pessoais ou base de dados a que tenham acesso para fins distintos da execução do contrato.

26.4. Caso o Contratado necessite coletar dados pessoais dos titulares mediante consentimento, indispensáveis a execução do contrato, esta será realizada após prévia aprovação do Contratante, sendo de sua exclusiva responsabilidade a obtenção e gestão desses dados.

26.5. Os dados obtidos em razão deste contrato deverão ser armazenados em banco de dados seguro, com garantia de registro das transações realizadas na aplicação de acesso (log), adequado controle baseado em função (*role based access control*) e com transparente identificação do perfil dos credenciados, como forma de garantir a rastreabilidade de cada transação e a franca apuração, a qualquer momento, de desvios e falhas, vedado o compartilhamento desses dados com terceiros.

26.6. O Contratado se responsabiliza integralmente pela regularidade do tratamento dos dados pessoais recebidos do Contratante ou gerados durante a execução do contrato, desde o momento do seu acesso ou coleta, até o seu descarte, devendo cumprir as regras impostas pela Lei Geral de Proteção de Dados, nos regulamentos dela decorrentes e orientações de boas práticas publicadas pela Autoridade Nacional de Proteção de Dados.

26.7. O Contratado obriga-se a implementar medidas técnicas e administrativas aptas a promover a segurança, à proteção, a confidencialidade e o sigilo da informação, dados pessoais e/ou base de dados que tenha acesso, a fim de evitar acessos não autorizados, acidentes, vazamentos acidentais ou ilícitos que causem destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito.

26.8. O Contratado é responsável por assegurar que seus colaboradores, consultores, e/ou prestadores de serviços que, no exercício de suas atividades, tenham acesso e/ou conhecimento da informação e/ou dos dados pessoais, respeitem o dever de proteção, confidencialidade e sigilo, devendo estes assumir compromisso formal de preservar a confidencialidade e segurança de tais dados.

26.9. O Contratado deverá manter os registros de tratamento de dados pessoais que realizar em razão do contrato, assim como aqueles compartilhados, com condições de rastreabilidade e de prova eletrônica a qualquer tempo.

26.10. O Contratado deverá permitir a realização de auditorias pelo Contratante e disponibilizar as informações necessárias para demonstrar o cumprimento das obrigações relacionadas à Lei Geral de Proteção de Dados.

26.11. O Contratado deverá prestar, sempre que solicitado pelo Contratante, qualquer informação e documentação que comprovem a implementação dos requisitos de segurança especificados na contratação, de forma a assegurar a auditabilidade do objeto contratado, bem como os demais dispositivos legais aplicáveis.

26.12. Em casos de incidentes de segurança, o Contratado informará imediatamente via e-mail e telefone ao fiscal do contrato o ocorrido, devendo a comunicação conter, no mínimo, as seguintes informações:

26.12.1. Identificação e dados de contato de entidade ou pessoa responsável pelo tratamento; encarregado de dados ou outra pessoa de contato; indicação se a notificação é completa ou parcial. Em caso de comunicação parcial, indicar que se trata de uma comunicação preliminar ou de uma comunicação complementar;

26.12.2. Informações sobre o incidente de segurança com dados pessoais, tais como data e hora da ocorrência e duração do incidente, bem como de sua detecção;

26.12.3. A natureza da violação de segurança de dados pessoais, como por exemplo, perda, roubo, cópia, vazamento, dentre outros;

26.12.4. Descrição dos dados pessoais e informações afetadas, como natureza e conteúdo dos dados pessoais, categoria e quantidade de dados e de titulares afetados;

26.12.5. Indicação da localização física, meio de armazenamento e base de dados violada;

26.12.6. Possíveis consequências e efeitos negativos sobre os titulares dos dados afetados, indicando os titulares atingidos ou potencialmente atingidos;

26.12.7. Medidas de segurança, técnicas e administrativas preventivas tomadas pelo Controlador de acordo com a LGPD aplicadas ao incidente;

26.12.8. Resumo das medidas implementadas durante o processo de adequação e *compliance* com a LGPD para mitigação de riscos de incidentes desta natureza;

26.12.9. Outras informações úteis às pessoas afetadas para proteger seus dados ou prevenir possíveis danos.

26.13. Extinto o contrato, o Contratado interromperá o tratamento dos dados pessoais que porventura viesse ocorrendo em função do contrato, devendo eliminá-los no prazo máximo 30 dias, salvo quando tenha que mantê-los para cumprimento de obrigação legal.

26.14. O Contratado é responsável pelos eventuais danos e sanções aplicadas pela Autoridade Nacional de Proteção de Dados, decorrentes do tratamento inadequado dos dados pessoais compartilhados pelo Contratante em razão do contrato.

26.15. O Contratado é responsável pelos danos patrimoniais, morais, individuais ou coletivos que venham a ser causados em razão do descumprimento de suas obrigações legais no processo de tratamento dos dados no âmbito do contrato.

27. ADEQUAÇÃO ORÇAMENTÁRIA

A despesa decorrente da presente contratação correrá por conta da seguinte dotação:

- **Unidade Gestora:** Tribunal de Contas do Estado de Roraima
- **Projeto de Trabalho:** 01.032.002.2012.9900.
- **Fonte (s):** 1500.
- **Natureza da Despesa:** 3.3.90-40 - 3.3.90.40 – Serviços de Tecnologia da Informação e Comunicação.

28. EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

Portaria 1045/2025/TCERR (ep. 1092215).

Integrante Requisitante	Integrante Técnico	Integrante Administrativo		
WENDERSON ARAGÃO MANO Chefe de Divisão	JOPPER GABRIEL QUEIROZ CHAVES Chefe de Divisão	VLADIMIR MARTINI MACHADO Chefe de Divisão		
	CARLOS FERNANDO DE ARAUJO FREIRE Diretor de Tecnologia da Informação			

Anexo I - Especificações Técnicas do Objeto

ITEM	DESCRIÇÃO DA DEMANDA	UNIDADE	QUANTIDADE
1	Serviço de Gerenciamento de Tecnologia de Segurança de Rede (UTM-NGFW) , garantia e suporte técnico pelo período de 60 meses , com disponibilidade de 2 equipamentos em regime de comodato.	Serv./mês.	60
2	Serviço de Gerenciamento de Tecnologia de Segurança de Rede Aplicação WEB (WAF - Web Application Firewall) , garantia e suporte técnico pelo período de 60 meses , com disponibilidade de equipamentos em regime de comodato.	Serv./mês	60
3	Solução de Relatoria , garantia e suporte técnico pelo período de 60 meses .	Serv./mês	60
4	Serviço de Implantação, Migração e Configuração.	Serv.	1
5	Serviço de Treinamento de equipe técnica do Contratante.	Serv.	1
6	Serviços Técnicos Especializados em Segurança da Informação (sob demanda)	UST	120

ITEM 01 - Serviço de Gerenciamento de Tecnologia de Segurança de Rede (UTM-NGFW), garantia e suporte técnico pelo período de 60 meses, com disponibilidade de 2 equipamentos em regime de comodato.

1. A solução deverá ser entregue em Alta Disponibilidade (HA);

- 1.1. Deve suportar, no mínimo, 23 (vinte e três) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;
- 1.2. Deve suportar, no mínimo, 6 (seis) milhões de conexões simultâneas;
- 1.3. Deve suportar, no mínimo, 200.000 (duzentas mil) novas conexões por segundo;
- 1.4. Deve suportar, no mínimo, 11,5 (onze e meio) Gbps de throughput VPN IPSec;
- 1.5. Deve estar licenciado para ou suportar, sem o uso de licença, no mínimo, 2.000 (dois mil) túneis de VPN IPSec Site-to-Site simultâneos;
- 1.6. Deve estar licenciado para ou suportar, sem o uso de licença, no mínimo, 15.000 (quinze mil) túneis de clientes VPN IPSec simultâneos;
- 1.7. Deve suportar, no mínimo, 9 (nove) Gbps de throughput de IPS;
- 1.8. Deve suportar, no mínimo, 7 (sete) Gbps de throughput de Inspeção SSL;
- 1.9. Deve suportar, no mínimo, 5 (cinco) Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS e antimalware;
- 1.10. Deve possuir, pelo menos, 8 (oito) interfaces Gigabit Ethernet com conectores RJ45;
- 1.11. Deve possuir, pelo menos, 8 (oito) interfaces com suporte a conectores SFP/SFP+ de 10 Gigabit Ethernet;
- 1.12. Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para gerenciamento;
- 1.13. Deve possuir, pelo menos, 1 (uma) interface RJ45 ou SFP/SFP+ dedicada para alta disponibilidade (HA);
- 1.14. Deve possuir unidade do tipo SSD com no mínimo 480GB para armazenamento de informações locais;
- 1.15. Deve possuir fonte de alimentação AC redundante;
- 1.16. Deve ser entregue pelo menos 8 (oito) transceivers ópticos por firewall, sendo 4 (quatro) do tipo 10GE SFP+ Short Range e 4 (quatro) do tipo 10GB SFP+ Long Range, ambos compatíveis e homologados com o

equipamento. Além disso, devem ser fornecidos 16 (dezesesseis) cabos compatíveis com os equipamentos e transceivers fornecidos nesta contratação, com comprimento de 3 metros;

1.17. Deve possuir, para os casos de appliances físicos, serviço de RMA com entrega de equipamentos e peças em até 5 (cinco) dias úteis após o diagnóstico.

2. CARACTERÍSTICAS GERAIS PARA FIREWALLS DE PRÓXIMA GERAÇÃO

2.1. A solução deve consistir em plataforma de proteção e balanceamento inteligente de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), console de gerência e monitoração;

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

2.3. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

2.4. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;

2.5. As funcionalidades de proteção de rede que compõe a solução de segurança, podem funcionar em múltiplos appliances desde que atendam a todos os requisitos desta especificação;

2.6. Deverá possuir e estar licenciado pelo período de 60 (sessenta) meses com as seguintes funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPsec, Controle de Aplicações, Prevenção de Perda de Dados (DLP) e Virtualização.

3. FUNCIONALIDADES DE REDE E FIREWALL

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

3.2. Os dispositivos de proteção de rede devem possuir suporte a VLANs;

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

3.4. Os dispositivos de proteção de rede devem possuir suporte a DHCP Cliente, Server e Relay;

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

3.6. Deve possuir a funcionalidade de tradução de endereços estáticos - NAT (Network Address Translation), um para um (1-to-1), N-para-um (N-to-1), vários para um, NAT64, NAT66, NAT46 e PAT;

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

3.8. Deverá suportar sFlow ou Netflow;

3.9. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;

3.10. Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;

3.11. Deve suportar o protocolo padrão da indústria VXLAN;

3.12. Deve implementar o protocolo ECMP;

3.13. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;

3.14. Enviar log para sistemas de monitoração externos;

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

3.16. Deve possuir mecanismos de proteção anti-spoofing;

3.17. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP4 e OSPFv2);

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

3.19. Suportar OSPF graceful restart;

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

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

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

- 3.23. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;
- 3.24. A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado às políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs e Tabelas FIB;
- 3.25. Deverá possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;
- 3.26. O modo de Alta-Disponibilidade (HA) deve possibilitar monitoração de falha de link;
- 3.27. A solução deve suportar obtenção de certificados válidos;
- 3.28. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls⁶¹. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;
- 3.29. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;
- 3.30. Deverá suportar controle por zonas de segurança;
- 3.31. Deverá suportar controles de políticas por porta e protocolo;
- 3.32. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;
- 3.33. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
- 3.34. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);
- 3.35. Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);
- 3.36. Deve descriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;
- 3.37. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;
- 3.38. Suporte a objetos e regras IPV6;
- 3.39. Suporte a objetos e regras multicast;
- 3.40. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

4. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

- 4.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
- 4.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
- 4.3. Reconhecer pelo menos 4.000 (quatro mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
- 4.4. Deverá possuir, pelo menos, 15 (quinze) categorias para classificação de aplicações;
- 4.5. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, Idap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
- 4.6. Deve inspecionar o payload de pacotes de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
- 4.7. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
- 4.8. Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

- 4.9. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação;
- 4.10. Identificar o uso de táticas evasivas via comunicações criptografadas;
- 4.11. Atualizar a base de assinaturas de aplicações automaticamente;
- 4.12. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
- 4.13. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
- 4.14. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
- 4.15. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;
- 4.16. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 4.17. Deve alertar o usuário quando uma aplicação for bloqueada;
- 4.18. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
- 4.19. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc.) possuindo granularidade de controle/políticas para os mesmos;
- 4.20. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc.) possuindo granularidade de controle/políticas para os mesmos;
- 4.21. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browser Based, Network Protocol, etc);
- 4.22. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, fabricante e popularidade;
- 4.23. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
- 4.24. Deve permitir forçar o uso de portas específicas para determinadas aplicações;

5. FUNCIONALIDADE DE PREVENÇÃO DE INTRUSÃO E AMEAÇAS

- 5.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;
- 5.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
- 5.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
- 5.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;
- 5.5. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
- 5.6. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- 5.7. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;
- 5.8. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- 5.9. Deve permitir o bloqueio de vulnerabilidades;
- 5.10. Deve permitir o bloqueio de exploits conhecidos;
- 5.11. Deve incluir proteção contra-ataques de negação de serviços;

- 5.12. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
- 5.13. Detectar e bloquear a origem de portscans;
- 5.14. Bloquear ataques efetuados por worms conhecidos;
- 5.15. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
- 5.16. Possuir assinaturas para bloqueio de ataques de buffer overflow;
- 5.17. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
- 5.18. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
- 5.19. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB/CIFS, SMTP e POP3;
- 5.20. Identificar e bloquear comunicação com botnets;
- 5.21. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 5.22. Os eventos devem identificar o país de onde partiu a ameaça;
- 5.23. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
- 5.24. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
- 5.25. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;
- 5.26. A solução deve ter capacidade de enviar artefatos suspeitos para serem executados em ambiente controlado na nuvem do fabricante;
- 5.27. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
- 5.28. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;

6. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB E DNS

- 6.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 6.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;
- 6.3. 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;
- 6.4. Deve permitir que os usuários sejam identificados através de consulta em uma base do Active Directory, permitindo que sua autenticação no domínio, não seja solicitada novamente para navegar através da solução;
- 6.5. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 6.6. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
- 6.7. Possuir pelo menos 80 (oitenta) categorias de URLs;
- 6.8. Deve possuir a função de exclusão de URLs do bloqueio;
- 6.9. Permitir a customização de página de bloqueio;
- 6.10. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;
- 6.11. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos e Comando e Controle (C&C) de botnets conhecidas;
- 6.12. Deve possuir filtro de domínio DNS baseado em categorias para inspecionar o tráfego DNS com classificação de domínios continuamente atualizado;

7. FUNCIONALIDADE DE IDENTIFICAÇÃO DE USUÁRIOS

- 7.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, eDirectory e base de dados local;
- 7.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 7.3. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2022 ou superior;
- 7.4. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;
- 7.5. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 7.6. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
- 7.7. 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 firewall (Captive Portal);
- 7.8. Deve suportar o envio e recebimento de credenciais via RADIUS;
- 7.9. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

8. FUNCIONALIDADE DE FILTRO DE DADOS

- 8.1. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP);
- 8.2. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 8.3. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 8.4. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

9. FUNCIONALIDADE DE GEOLOCALIZAÇÃO

- 9.1. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;
- 9.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

10. FUNCIONALIDADE DE VPN

- 10.1. Suportar VPN Site-to-Site e Client-To-Site;
- 10.2. Suportar IPSec VPN;
- 10.3. A VPN IPSEC deve suportar 3DES;
- 10.4. A VPN IPSEC deve suportar Autenticação MD5 e SHA-1;
- 10.5. A VPN IPSEC deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
- 10.6. A VPN IPSEC deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
- 10.7. A VPN IPSEC deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
- 10.8. A VPN IPSEC deve suportar Autenticação via certificado IKE PKI;
- 10.9. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
- 10.10. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
- 10.11. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução,

facilitando o processo de troubleshooting;

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

10.13. Atribuição de DNS nos clientes remotos de VPN;

10.14. Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, AntiSpyware e filtro de URL para tráfego dos clientes remotos conectados na VPN;

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

10.16. Suportar leitura e verificação de CRL (Certificate Revocation List);

10.17. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulem dentro dos túneis VPN;

10.18. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Após autenticação do usuário na estação;

10.19. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Sob demanda do usuário;

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

10.21. O agente de VPN client-to-site deve ser compatível com pelo menos: Windows (10 ou superior), Ubuntu Linux (22.04 ou superior), Red Hat Linux (7.4 ou superior), Fedora Linux (36 ou superior) e macOS (v13 ou superior).

11. FUNCIONALIDADE DE QOS, TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

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

11.2. Suportar a criação de políticas de QoS e Traffic Shaping para os seguintes itens:

11.2.1. Endereço de origem;

11.2.2. Endereço de destino;

11.2.3. Usuário e grupo;

11.2.4. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube;

11.2.5. Por porta;

11.3. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;

11.4. O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como YouTube, Facebook, entre outros;

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

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

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

11.8. Suportar modificação de valores DSCP para o Diffserv;

11.9. Suportar priorização de tráfego usando informação de ToS (Type of Service);

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

11.11. Deve suportar QoS (Traffic-Shapping), em interface agregadas ou redundantes;

11.12. Deve possibilitar a definição de bandas distintas para download e upload;

12. FUNCIONALIDADE DE BALANCEAMENTO INTELIGENTE DE LINKS

12.1. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;

12.2. A solução deve ser capaz de agregar vários links em uma interface virtual;

12.3. A solução deve ser possível criar políticas de roteamento inteligente, mediante regras pré-estabelecidas considerando a verificação das seguintes condições: Endereços de origem, Grupos de usuários, Endereços de destino, Serviços na Internet e Aplicações de camada 7 (0365 Exchange, AWS, Dropbox e etc);

12.4. A solução deve ser capaz de medir o status de qualidade do link baseando-se em critérios mínimos de latência, jitter e perda de pacotes, onde deve ser possível configurar um valor limite para cada um destes itens que será utilizado como gatilho para fator de decisão nas regras de tráfego de saída e balanceamento inteligente;

12.5. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de balanceamento em condições em que a largura de banda é modificada;

12.6. A solução deve ser capaz de monitorar a qualidade e identificar falhas nos links, enviando sinais por meio de cada link para servidores ou aplicações, permitindo utilizar protocolos como Ping, HTTP, TCP ECHO, UDP ECHO, DNS, TCP Connect e TWAMP (Two-way Active Measurement Protocol). Deve suportar ainda um método para mensurar a qualidade do tráfego de voz corporativo;

12.7. A solução deve possibilitar balanceamento de tráfego entre conexões WAN, de forma em que o algoritmo de balanceamento de carga utilizado possa ser configurado considerando os seguintes parâmetros: Sessões, Volume de tráfego, IP de origem e destino e Transbordo de link (Spillover).

12.8. A solução deve possibilitar a criação de regras para seleção das interfaces e suas prioridades que serão utilizadas para encaminhar o tráfego de saída da rede, considerando os seguintes critérios:

12.8.1. Manual: Deve permitir que as interfaces tenham as prioridades atribuídas manualmente.

12.8.2. Melhor Qualidade: Deve permitir que as interfaces recebam uma prioridade com base na qualidade do link no qual a interface está conectada, considerando o monitoramento de um dos seguintes parâmetros com valores customizáveis: latência, jitter, perda de pacotes ou largura de banda;

12.8.3. Menor Custo: Deve permitir que as interfaces recebam uma prioridade com base no custo atribuído a interface, considerando a satisfação dos parâmetros de qualidade do link no qual a interface está conectada;

12.8.4. Balanceamento de Carga: Deve permitir que o tráfego seja distribuído entre todas as interfaces disponíveis com base em algoritmos de balanceamento de carga e satisfação dos parâmetros customizados de qualidade do link no qual a interface está conectada;

12.9. A solução de balanceamento inteligente deve suportar marcação de pacotes DSCP nas definições e regras para o tráfego balanceado;

12.10. A solução de balanceamento inteligente de links deve suportar Roteamento dinâmico (OSPFv2/v3, BGPv4/BGP4+);

12.11. A solução deve realizar o reconhecimento de aplicações, em camada 7, de pelo menos 3.000 (três mil) aplicações, incluindo Aplicações SaaS, em Nuvem e Multimídia (Vimeo, YouTube, Facebook, etc);

12.12. Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos;

12.13. A solução deve possibilitar a criação e uso de túneis VPN de forma dinâmica entre unidades remotas, para aplicações sensíveis. Uma vez que as unidades trocam informações entre si, o tráfego deve ser encaminhado diretamente entre as unidades remotas sem passar pela unidade Sede;

12.14. A solução deve permitir a duplicação de pacotes entre dois ou mais links, que atendam os parâmetros de qualidade estabelecidos, objetivando uma melhor experiência de uso de aplicações;

12.15. A solução deve possuir recurso para controlar e corrigir erros (FEC) na transmissão de dados, enviando dados redundantes através de túnel VPN em antecipação à perda de pacotes que pode ocorrer durante o trânsito;

12.16. A solução deve permitir a customização de intervalo de tempo em que é feita a verificação da situação de um link, assim como, permitir definir a quantidade de falhas encontradas no link antes de declará-lo inativo, com objetivo de identificar oscilações nos links, que possam impactar os serviços e a experiência dos usuários;

12.17. A solução deve suportar nativamente conectores com clouds públicas;

12.18. Deve possibilitar a definição de largura de banda distintas nas interfaces para download e upload;

12.19. A solução deve prover estatísticas em tempo real a respeito da utilização da largura de banda (upload e download) e nível de qualidade dos links (perda de pacote, jitter e latência);

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

- 12.21. Deve implementar balanceamento de link por hash do IP de origem e destino;
- 12.22. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;
- 12.23. Deve ser possível extrair informações de desempenho das verificações de saúde mediante REST API, permitindo assim a consolidação de tais informações em alguma aplicação terceira.

13. FUNCIONALIDADES CAPTIVE PORTAL

- 13.1. A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informar as credenciais válidas para acesso à rede;
- 13.2. A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;
- 13.3. A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;
- 13.4. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;
- 13.5. A solução deve permitir que a página de autenticação seja hospedada em servidor externo;
- 13.6. A solução deve permitir a configuração do captive portal com endereço IPv6;
- 13.7. A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;
- 13.8. A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;
- 13.9. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;
- 13.10. A solução deve implementar recurso de DHCP Server (em IPv4 e IPv6) para facilitar a configuração de redes visitantes;
- 13.11. A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;
- 13.12. A solução deve permitir o envio dos logs para servidores syslog externos;

14. FUNCIONALIDADE DE CONTROLADOR DE REDE CABEADA

- 14.1. Deve operar como ponto central para automação e gerenciamento dos switches deste termo, sendo permitido o atendimento através de composição de solução do mesmo fabricante que possua gerência centralizada para switches, devendo atender aos requisitos descritos abaixo:
 - 14.1.1. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches;
 - 14.1.2. Deve possuir interface gráfica para configuração, administração e monitoração dos switches;
 - 14.1.3. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede;
 - 14.1.4. Deve montar a topologia da rede de maneira automática;
 - 14.1.5. Deve ser capaz de configurar os switches da rede;
 - 14.1.6. Através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribuí-las automaticamente em todos os switches gerenciados;
 - 14.1.7. Através da interface gráfica deve ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;
 - 14.1.8. Através da interface gráfica deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;
 - 14.1.9. Através da interface gráfica deve ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;
 - 14.1.10. Através da interface gráfica deve ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches;

- 14.1.11. Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;
- 14.1.12. Através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard;
- 14.1.13. Através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;
- 14.1.14. A solução deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection);
- 14.1.15. Deve ser capaz de configurar parâmetros SNMP dos switches;
- 14.1.16. A solução deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente;
- 14.1.17. A solução deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas;
- 14.1.18. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica;
- 14.1.19. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches;
- 14.1.20. A solução deve apresentar graficamente informações sobre disponibilidade dos switches;
- 14.1.21. Deve prover indicadores de saúde dos elementos críticos do ambiente;
- 14.1.22. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;
- 14.1.23. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede;

ITEM 02 - Serviço de Gerenciamento de Tecnologia de Segurança de Rede Aplicação WEB (WAF - Web Application Firewall), garantia e suporte técnico pelo período de 60 meses, com disponibilidade de equipamentos em regime de comodato.

1. REQUISITOS MÍNIMOS DE FUNCIONALIDADE

- 1.1. A solução deve possuir softwares específicos, e hardware dedicado para os itens de appliance físico, destinados à finalidade de Firewall de Aplicação Web (WAF), bem como as licenças necessárias, conforme requerido neste termo de referência, para o seu funcionamento e proteção de servidores e aplicações Web;
- 1.2. Deve possuir garantia, suporte técnico, suporte a atualizações e estar licenciado com as funcionalidades descritas neste termo pelo período de 60 (sessenta) meses;
- 1.3. Deve possuir, para os casos de appliances físicos, serviço de RMA com entrega de equipamentos e peças em até 5 (cinco) dias úteis após o diagnóstico;
- 1.4. Em caso de defeitos em peças/dispositivos que possuam armazenamento de dados, o serviço de RMA deve permitir a retenção, pelo cliente, dessas peças/dispositivos defeituosos, a fim de garantir o sigilo dos dados pessoais e dos dados críticos para o governo ali armazenados.

2. FUNCIONALIDADES DE REDE

- 2.1. A solução deve ser capaz de ser implementada no modo Proxy (Transparente e Reverso), Passivo e Inline Transparente (Bridge);
- 2.2. A solução deve ser capaz de implementar protocolos de redirecionamento de tráfego transparente;
- 2.3. Suportar VLANs no padrão IEEE 802.1q;
- 2.4. Deve implementar o protocolo de negociação Link Aggregation Control Protocol (LACP) - IEEE 802.3ad;
- 2.5. Suportar endereçamento IPv4 e IPv6 nas interfaces físicas e virtuais (VLANs);
- 2.6. A solução ofertada deve oferecer suporte a cluster de alta disponibilidade entre dois dispositivos no modo Ativo- Passivo e Ativo-Ativo, para que quando o principal falhar o tráfego possa continuar sendo processado;
- 2.7. A solução deve suportar a sincronização de configuração entre dois appliances iguais, com o objetivo de

operar no modo ativo-ativo, com a distribuição de tráfego sendo realizada por balanceador de carga externo ou pela própria solução;

2.8. A solução deve suportar roteamento por política (policy route).

3. FUNCIONALIDADES DE GERÊNCIA

3.1. O sistema operacional / firmware deve suportar interface gráfica web para a configuração das funções do sistema operacional, utilizando navegadores disponíveis gratuitamente e protocolo HTTPS, e através de CLI (interface de linha de comando), acessando localmente, via porta de console, ou remotamente via SSH;

3.2. Deve possuir administração baseada em interface web HTTPS;

3.3. Possuir auto-complementação de comandos na CLI;

3.4. Possuir ajuda contextual na CLI;

3.5. A solução deve possuir Interface Gráfica com informações sobre o sistema, Ex: (Informações do Cluster, hostname, número de série, modo de operação, tempo em serviço, versão do firmware);

3.6. Deverá ser possível visualizar através da interface gráfica de gerência informações de licenças e assinaturas;

3.7. Deve prover, na interface de gerência, as seguintes informações do sistema para cada gateway: consumo de CPU e estatísticas das conexões;

3.8. Deve ser possível visualizar na interface de gerência as informações de consumo de memória;

3.9. Deve ser possível visualizar na interface de gerência ou CLI as informações de utilização de disco de log;

3.10. Deverá possuir ferramenta, na interface gráfica de gerência (dashboard) que permita visualizar os últimos logs de ataque detectados/bloqueados;

3.11. Deve prover as seguintes informações, na interface de gráfica de gerência: estatísticas de throughput HTTP em tempo real, estatísticas dos eventos de ataque detectados/bloqueados, estatísticas de requisições HTTP em tempo real e últimos logs de eventos do sistema;

3.12. Possui na interface gráfica estatísticas de conexões concorrentes e por segundo, de políticas de segurança do sistema;

3.13. Possui um painel de visualização com informações das interfaces de rede do sistema;

3.14. A configuração de administração da solução deve possibilitar a utilização de perfis;

3.15. Deve ser possível executar e restaurar backup via interface Web (GUI);

3.16. Deve ter a opção para criptografar o backup;

3.17. Deve ser possível executar e restaurar backup utilizando-se um ou mais dos seguintes protocolos: FTP, SFTP ou TFTP;

3.18. Deve ser possível instalar um firmware alternativo em disco e inicializá-lo em caso de falha do firmware principal;

3.19. Deve ter suporte ao protocolo de monitoração SNMP v1, SNMP v2c e SNMP v3;

3.20. Deve ser capaz de realizar notificações de eventos de segurança através de e-mail, traps SNMP e Syslog;

3.21. A solução deverá ter a capacidade de armazenar logs localmente em disco e em servidor externo via protocolo SYSLOG;

3.22. Ter a capacidade de armazenar logs em appliance remoto;

3.23. A solução deve ter a capacidade de enviar alertas por e-mail de eventos baseados em severidades e/ou categorias;

3.24. A solução deve possuir dados analíticos contendo localização geográfica dos clientes web;

3.25. A solução deve possuir dados analíticos, sendo possível visualizar a contagem total de ataques e percentual de cada país de origem, o volume total de tráfego em bytes e percentual de cada país de origem e o total de acessos (hits) e percentual de cada país de origem;

3.26. Deverá ter a capacidade de gerar relatórios detalhados baseados em tráfego/acessos/atividades do usuário;

3.27. Deve ter suporte a RESTful API para gerenciamento de configurações.

4. FUNCIONALIDADES DE AUTENTICAÇÃO

- 4.1. Os usuários devem ser capazes de autenticar através do cabeçalho de autorização HTTP/HTTPS;
- 4.2. Os usuários devem ser capazes de autenticar através de formulários HTML embutidos;
- 4.3. A solução deverá ser capaz de autenticar usuários através de certificados digitais pessoais;
- 4.4. Deve possuir base local para armazenamento e autenticação contas de usuários;
- 4.5. A solução deve ter a capacidade de autenticar usuários em bases externas/remotas LDAP e RADIUS;
- 4.6. Os usuários devem ser capazes de autenticar através de contas de usuários em base remota NTLM;
- 4.7. A solução deve ser capaz de criar grupos de usuários para acessos semelhantes na autenticação;

5. FUNCIONALIDADE DE FIREWALL DE APLICAÇÃO (WAF)

- 5.1. Deverá ser capaz de identificar e bloquear ataques através de um banco de dados de assinaturas de vírus e IP reputation, atualizado de forma automática;
- 5.2. Deverá implementar recurso de machine learning, onde será permitido implementar proteção para um servidor ou grupo de servidores de aplicação web, de forma automatizada através da análise da utilização da aplicação, fazendo a descoberta da estrutura e padrões e padrões de uso, buscando separar o comportamento anormal do abusivo, detectando anomalias e tentativas de ataque;
- 5.3. Ter a capacidade de criação de assinaturas de ataque customizáveis;
- 5.4. Ter a capacidade de proteção para ataques do tipo Adobe Flash binary (AMF) protocol;
- 5.5. Ter a capacidade de proteção para ataques do tipo Botnet;
- 5.6. Ter a capacidade de proteção para ataques do tipo Browser Exploit Against SSL/TLS (BEAST);
- 5.7. A solução deverá possuir funcionalidade de proteção ativa ataques como acesso por força bruta;
- 5.8. Deve suportar detecção de ataques de Clickjacking;
- 5.9. Deve suportar detecção a ataques de alteração de cookie;
- 5.10. Identificar e prevenir ataques do tipo Credit Card Theft;
- 5.11. Identificar e prevenir ataque Cross Site Request Forgery (CSRF);
- 5.12. A solução deverá possuir funcionalidade de proteção ativa contra ataques como cross site scripting (XSS);
- 5.13. Deve possuir proteção contra ataques de Denial of Service (DoS);
- 5.14. Ter a capacidade de proteção para ataques do tipo HTTP header overflow;
- 5.15. Ter a capacidade de proteção para ataques do tipo Local File inclusion (FLI);
- 5.16. Ter a capacidade de proteção para ataques do tipo Man-in-the-middle (MITM);
- 5.17. Ter a capacidade de proteção para ataques do tipo Remote File Inclusion (RFI);
- 5.18. Ter a capacidade de proteção para ataques do tipo Server Information Leakage;
- 5.19. Proteção contra envios de comandos SQL escondidos nas requisições enviadas a bases de dados (SQL Injection);
- 5.20. Ter a capacidade de proteção para ataques do tipo Malformed XML;
- 5.21. Identificar e prevenir ataques do tipo Low-rate DoS;
- 5.22. Prevenção contra Slow POST attack;
- 5.23. Proteger contra ataques Slowloris;
- 5.24. Ter a capacidade de proteção para ataques do tipo SYN flood;
- 5.25. Ter a capacidade de proteção para ataques do tipo Forms Tampering;
- 5.26. A solução deverá possuir funcionalidade de proteção ativa contra ataques de manipulação de campo escondido;
- 5.27. Ter a capacidade de proteção para ataques do tipo Directory Traversal;
- 5.28. Ter a capacidade de proteção do tipo Access Rate Control;
- 5.29. Ter a habilidade de configurar proteção do tipo TCP SYN flood-style para prevenção de DoS para

qualquer política, através de Syn Cookie e Half Open Threshold;

5.30. Permitir configurar regras de bloqueio a métodos HTTP indesejados;

5.31. Permitir que sejam configuradas regras de limite de upload por tamanho de arquivo;

5.32. Deve permitir que o administrador bloqueie o tráfego de entrada e/ou tráfego de saída com base nos países, sem a necessidade de gerir manualmente os ranges de endereços IP correspondentes a cada país;

5.33. Deve suportar a criação de políticas por geolocalização, permitindo que o tráfego de determinado país seja bloqueado;

5.34. Permitir configurar listas negras de bloqueio e listas brancas de confiança, baseadas em endereço IP de origem;

5.35. Permitir a liberação temporária ou definitiva (whitelist) de endereços IP bloqueados por terem originado ataques detectados pela solução;

5.36. Deve permitir adicionar, automaticamente ou manualmente, em uma lista de bloqueio, os endereços IP de origem, de acordo com a base de IP Reputation;

5.37. Ter a capacidade de Prevenção ao Vazamento de Informações (DLP), bloqueando o vazamento de informações de cabeçalho HTTP;

5.38. Ter a funcionalidade de proteger o website contra ações de desfiguração (defacement), com restauração automática e rápida do site caso ocorra à falha;

5.39. Ter a funcionalidade de antivírus para inspeção de tráfego e arquivos;

5.40. Ter a capacidade de investigar e analisar todo o tráfego HTTP para atestar se está em conformidade com a respectiva RFC, bloqueando ataques e tráfego em não-conformidade;

5.41. Deverá ser capaz de fazer aceleração de SSL, onde os certificados digitais são instalados na solução e as requisições HTTP são enviadas aos servidores sem criptografia;

5.42. A solução deve ser capaz de funcionar como Terminador de sessões SSL para a aceleração de tráfego;

5.43. Para SSL/TLS offload suportar no mínimo TLS 1.0, 1.1, 1.2 e 1.3;

5.44. A solução deve ter a capacidade de armazenar certificados digitais de CA's;

5.45. A solução deve ser capaz de gerar CSR para ser assinado por uma CA;

5.46. A solução deve ser capaz de validar os certificados que são válidos e não foram revogados por uma lista de certificados revogados (CRL);

5.47. A solução deve conter as assinaturas de robôs conhecidos como link checkers, indexadores de web, search engines, spiders e web crawlers que podem ser colocados nos perfis de controle de acesso, bem como resetar tais conexões;

5.48. A solução deve ter um sistema de reputação de endereços IP públicos conhecidos como fontes de ataques DDoS, botnets, spammers, etc. Tal sistema deve ser atualizado automaticamente;

5.49. A solução deverá ser capaz de limitar o total de conexões permitidas para cada servidor real de um pool de servidores;

5.50. A solução deve permitir a customização ou redirecionar solicitações e respostas HTTP no HTTP Host, Request URL HTTP, HTTP Referer, HTTP Body e HTTP Location;

5.51. A solução deve permitir criar regras definindo a ordem em que as páginas devem ser acessadas para prevenir ataques como cross-site request forgery (CSRF);

5.52. A solução deve ter a capacidade de definir restrições a métodos HTTP;

5.53. A solução deve ter a capacidade de proteger contra a detecção de campos ocultos;

5.54. Permitir que sejam criadas assinaturas customizadas de ataques e DLP, através de expressões regulares;

5.55. A solução deve incluir capacidade de atuar como um scanner de vulnerabilidades ou permitir a integração com scanners de vulnerabilidade de terceiros para diagnóstico e identificação de ameaças nos servidores web, software desatualizado e potenciais buffers overflows;

5.56. Deve gerar perfil de proteção automaticamente a partir de relatório em formato XML gerado por scanner de vulnerabilidade de terceiros;

5.57. A solução deve gerar um relatório da análise de vulnerabilidades no formato HTML;

- 5.58. A solução deve permitir a exclusão de URLs na análise de vulnerabilidades;
- 5.59. Deverá ser capaz de fazer compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;
- 5.60. Suportar redireção e reescrita de requisições e respostas HTTP;
- 5.61. Permitir redirecionar requisições HTTP para HTTPS;
- 5.62. Permitir reescrever a linha URL no cabeçalho de uma requisição HTTP;
- 5.63. Permitir reescrever o campo "Host:" no cabeçalho de uma requisição HTTP;
- 5.64. Permitir reescrever o campo "Referer:" no cabeçalho de uma requisição HTTP;
- 5.65. Permitir redirecionar requisições para outro web site;
- 5.66. Permitir enviar resposta HTTP 403 Forbidden para requisições HTTP;
- 5.67. Permitir reescrever o parâmetro "Location:" no cabeçalho HTTP de uma resposta de redireção HTTP de um servidor web;
- 5.68. Permitir reescrever o corpo ("body") de uma resposta HTTP de um servidor web;
- 5.69. Permitir adicionar o campo X-Forwarded-For para identificação do endereço real do cliente quando no modo de proxy reverso;
- 5.70. A solução deve suportar regras para definir se as solicitações HTTP serão aceitas com base na URL e a origem do pedido e, se necessário, aplicar uma taxa específica de transferência (rate limit);
- 5.71. A solução deve suportar o mecanismo de combinação de controle de acesso e autenticação utilizando mecanismos como HTML Form, Basic e Suporte a SSO, métodos como LDAP e RADIUS para consultas e integração dos usuários da aplicação;
- 5.72. Possuir capacidade de caching para aceleração web;
- 5.73. Deve permitir ao Administrador a criação de novas assinaturas e/ou alteração de assinaturas já existentes.

6. FUNCIONALIDADE DE BALANCEAMENTO DE CARGA

- 6.1. A solução deve incluir funcionalidade de balanceamento de carga entre servidores web;
- 6.2. Deve ter a habilidade de configurar portas não-padrão para aplicação web HTTP e HTTPS;
- 6.3. Ter a capacidade de balancear/distribuir tráfego e rotear o conteúdo através de vários servidores web;
- 6.4. A solução deve permitir criar grupos de servidores (Server Farm / Pool) para distribuir as conexões dos usuários;
- 6.5. Suportar algoritmo Round Robin para balanceamento de carga de servidores;
- 6.6. Suportar algoritmo Weighted Round Robin para balanceamento de carga de servidores;
- 6.7. Suportar algoritmo Least Connections para balanceamento de carga de servidores;
- 6.8. A solução deve ser capaz de criar servidores virtuais que definem a interface de rede/bridge e endereço IP por onde o tráfego destinado ao Server Pool é recebido;
- 6.9. Os servidores virtuais devem entregar o tráfego à um único servidor web e também possuir a opção de distribuir as sessões/conexões entre os servidores web do Server Pool;
- 6.10. Deve ser possível especificar o número máximo de conexões TCP simultâneas para um determinado servidor membro do Server Pool;
- 6.11. Permitir teste de disponibilidade de servidor web através do método TCP;
- 6.12. Permitir teste de disponibilidade de servidor web através do método ICMP ECHO_REQUEST (ping);
- 6.13. Permitir teste de disponibilidade de servidor web através do método TCP Half Open;
- 6.14. Permitir teste de disponibilidade de servidor web através do método TCP SSL3;
- 6.15. Permitir teste de disponibilidade de servidor web através do método HTTP;
- 6.16. Permitir teste de disponibilidade de servidor web através do método HTTPS;
- 6.17. Nos testes de disponibilidade HTTP e HTTPS, permitir indicar a URL exata a ser testada;
- 6.18. Nos testes de disponibilidade HTTP e HTTPS, permite escolher entre os métodos HEAD, GET e POST;

- 6.19. Nos testes de disponibilidade HTTP e HTTPS, permitir indicar o nome do campo HTTP "host" a ser testado;
- 6.20. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Host";
- 6.21. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "URL";
- 6.22. Suportar roteamento das requisições dos clientes web baseado "Parâmetro HTTP";
- 6.23. Suportar roteamento das requisições dos clientes web baseado "Referer";
- 6.24. Suportar roteamento das requisições dos clientes web baseado "Endereço";
- 6.25. Suportar roteamento das requisições dos clientes web baseado "Cabeçalho";
- 6.26. Suportar roteamento das requisições dos clientes web baseado "Cookie";
- 6.27. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Valor de campo do Certificado X509";
- 6.28. Implementar Cache de Conteúdo para HTTP, permitindo que objetos sejam armazenados e requisições HTTP sejam respondidas diretamente pela solução;
- 6.29. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por endereço IP de origem;
- 6.30. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência analisando qualquer parâmetro do header HTTP;
- 6.31. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência analisando a URL acessada;
- 6.32. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por cookie - método cookie insert e cookie rewrite;
- 6.33. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por embedded cookie (cookie original mais porção randômica);
- 6.34. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em Reescrita de Cookie;
- 6.35. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em Cookie Persistente;
- 6.36. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em ASP Session ID;
- 6.37. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em PHP Session ID;
- 6.38. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em JSP Session ID;
- 6.39. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por sessão SSL.

7. FUNCIONALIDADE DE PROTEÇÃO DE API

- 7.1. Fornecer proteção para a comunicação API, sejam elas implementadas usando XML, JSON API ou RESTful API;
- 7.2. Permitir a utilização de arquivos de esquema JSON para verificar o conteúdo JSON em solicitações HTTP, a fim de determinar o conteúdo aceitável e validar se o conteúdo está bem formado;
- 7.3. Permitir definir a limitação de parâmetros JSON tais como total de dados, tamanho da chave, total de chaves, entre outros;
- 7.4. Permitir ações do tipo alertar, bloquear, bloquear temporariamente, redirecionar ou responder com erro 403;
- 7.5. Permitir definir o nível de severidade dos logs das ações;
- 7.6. Permitir a utilização de arquivos de esquema XML para verificar o conteúdo XML em solicitações HTTP, a fim de determinar o conteúdo aceitável e validar se o conteúdo está bem formado;
- 7.7. Permitir definir a limitação de parâmetros XML tais como total de atributo, tamanho do nome do atributo, tamanho CDATA, entre outros;

- 7.8. Permitir definir elementos proibidos XML tais como entidade externa, XInclude, local do esquema, entre outros;
- 7.9. Permitir definir o seguinte formato do esquema: SOAP ou XML;
- 7.10. Permitir ações do tipo alertar, bloquear, bloquear temporariamente, redirecionar ou responder com erro 403;
- 7.11. Permitir definir o nível de severidade dos logs das ações;
- 7.12. Fornecer suporte a proteção OpenAPI;
- 7.13. Permitir o upload de arquivo de descrição OpenAPI, e bloquear as solicitações que não correspondam às definições do arquivo;
- 7.14. Suportar a proteção de API Móvel;
- 7.15. Permitir a verificação de flags de API móvel e com a regra de proteção de API configuradas, executar as ações definidas na regra de proteção;
- 7.16. Permitir ações do tipo alertar, bloquear, bloquear temporariamente, entre outras;
- 7.17. Permitir definir o nível de severidade dos logs das ações;
- 7.18. Suportar as seguintes funções de API gateway:
- 7.19. Gerenciamento de usuários API;
- 7.20. Verificação de chave API;
- 7.21. Controle de acesso API;
- 7.22. Controle de limite de taxa;
- 7.23. Reescrita de chamada de API;
- 7.24. Permitir definir usuários de API para restringir o acesso a APIs com base em chaves de API;
- 7.25. Permitir a restrição baseada em endereçamento IP;
- 7.26. Permitir a restrição baseada em referenciadores HTTP;
- 7.27. Permitir a criação de grupos de usuários;
- 7.28. Permitir restringir o acesso à API através de regras envolvendo verificação de chave API, transferência de chave API, agrupamento de usuários API, configuração de subURL e ações específicas de qualquer violação de chamada API.

8. REQUISITOS TÉCNICOS ESPECÍFICOS PARA SOLUÇÃO DE PROTEÇÃO DE APLICAÇÕES WEB E API (WAAP)

- 8.1. Deve ser do tipo appliance físico com software e recurso dedicado à função de Firewall de Aplicação (WAF);
- 8.2. Deve oferecer cluster de alta disponibilidade entre dois dispositivos no modo Ativo-Passivo e Ativo-Ativo, para que quando o principal falhar o tráfego possa continuar sendo processado;
- 8.3. Deve possuir throughput mínimo para tráfego HTTPS, com chave de 2048 bytes, de 500 (quinhentos) Mbps;
- 8.4. Deve introduzir latência inferior a 5 milissegundos, a fim de não impactar o desempenho das aplicações Web;
- 8.5. Deve suportar quantidade ilimitada de aplicações protegidas;
- 8.6. Deve possuir, pelo menos, 4 (quatro) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;
- 8.7. Deve possuir 04 (quatro) interfaces Gigabit Ethernet com conectores SFP;
- 8.8. Deve possuir fonte de alimentação bivolt (100/240V);
- 8.9. Deve possuir área de armazenamento com no mínimo 1 (um) SSD de 480 (quatrocentos e oitenta) GB;
- 8.10. Deve suportar no mínimo 30 (trinta) instâncias administrativas independentes entre si, permitindo criar níveis diferentes de privilégios de acesso dos administradores;
- 8.11. Deve suportar no mínimo 60 (sessenta) políticas de servidores;
- 8.12. Deve suportar no mínimo 200 (duzentos) grupos ou pools de servidores, e cada pool deve suportar no

mínimo 1000 (mil) membros;

8.13. Deve suportar no mínimo 500(quinhentos) IPs virtuais configurados e ativos simultaneamente;

8.14. Deve Possuir LEDs para a indicação do status e atividade das interfaces.

ITEM 3 - Solução de Relatoria, garantia e suporte técnico pelo período de 60 meses.

1. CARACTERÍSTICAS GERAIS PARA GERENCIAMENTO CENTRALIZADO DE LOGS E RELATORIA:

- 1.1. Deve suportar o acesso via SSH, WEB (HTTPS) para gerenciamento da solução;
- 1.2. A solução de gerenciamento centralizado poderá ser ofertada em formato de appliance físico ou appliance virtual, e caso ofertado em formato virtual, será responsabilidade da contratante a disponibilização dos recursos de hardware e software (hypervisor) necessário para funcionamento da solução;
- 1.3. Caso a solução seja entregue em appliance virtual, deverá ser compatível com Hypervisors: VMware ESXi 6.5, Microsoft Hyper-V 2022 ou superior, KVM no Redhat 7.1 e Nutanix AHV 5.10 ou superior;
- 1.4. Caso a solução seja entregue em appliance virtual, não deve possuir limite na quantidade de múltiplas vCPU;
- 1.5. Caso a solução seja entregue em appliance virtual, não deve possuir limite para suporte a expansão de memória RAM;
- 1.6. Caso a solução seja ofertada em appliance físico, deverá ser em hardware do próprio fabricante;
- 1.7. A solução deverá estar devidamente licenciada com suporte durante todo o tempo de contrato;
- 1.8. A solução deverá ser capaz de armazenar logs por no mínimo 12 (doze) meses;
- 1.9. Permitir acesso simultâneo à administração, bem como criar pelo menos 2 (dois) perfis para administração e monitoramento;
- 1.10. Possuir suporte para SNMP versão 2 e 3;
- 1.11. Permitir a virtualização do gerenciamento e administração dos dispositivos, onde cada administrador tem acesso apenas aos equipamentos autorizados;
- 1.12. Deve permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução;
- 1.13. Suporte a definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais;
- 1.14. Suporte a autenticação de usuários de acesso à plataforma via LDAP, Radius ou TACACS+;
- 1.15. Deve suportar a configuração Master / Slave de alta disponibilidade em camada 3;
- 1.16. Deve permitir gerar alertas de eventos a partir de logs recebidos;
- 1.17. A solução deve ter relatórios predefinidos;
- 1.18. Permitir importação e exportação de relatórios
- 1.19. Suporte a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;
- 1.20. Suporte a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;
- 1.21. Suporte a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;
- 1.22. Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;
- 1.23. Deve ter a capacidade de personalizar a capa dos relatórios obtidos;
- 1.24. Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;
- 1.25. Deve ter a capacidade de criar relatórios no formato HTML, CSV, XML e PDF;
- 1.26. Deve conter um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha;
- 1.27. Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;

- 1.28. Deve possuir mecanismos de remoção automática para logs antigos;
- 1.29. Deve ter um mecanismo de "pesquisa detalhada" ou "Drill-Down" para navegar pelos relatórios em tempo real;
- 1.30. Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;
- 1.31. Permitir o envio por e-mail relatórios automaticamente;
- 1.32. Deve permitir que o relatório seja enviado por Email para o destinatário específico;
- 1.33. Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;
- 1.34. Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado;
- 1.35. Deve permitir o uso de filtros nos relatórios;
- 1.36. Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;
- 1.37. Permitir especificar o idioma dos relatórios criados;
- 1.38. Gerar alertas automáticos via e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;
- 1.39. Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;
- 1.40. Deve permitir o envio automático dos logs para um servidor FTP externo a solução;
- 1.41. Deve permitir exportar os logs no formato CSV;
- 1.42. Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;
- 1.43. Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;
- 1.44. Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;
- 1.45. Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;
- 1.46. Possibilidade de exibir nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;
- 1.47. Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;
- 1.48. Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;
- 1.49. Deve permitir visualizar em tempo real os logs recebidos;
- 1.50. Deve permitir o encaminhamento de log no formato syslog e CEF (Common Event Format);
- 1.51. Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs;
- 1.52. Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;
- 1.53. Deve possuir um painel de operações que monitore as principais ameaças à segurança da sua rede;
- 1.54. Deve possuir um painel de operações que monitorea o envolvimento do usuário e o uso suspeito da web em sua rede;
- 1.55. Deve possuir um painel de operações que monitora o tráfego da rede, aplicativos e sites web;
- 1.56. Deve possuir um painel de operações que monitoram a atividade da VPN em sua rede;
- 1.57. Deve possuir um painel de operações que monitoram o desempenho dos recursos locais da solução (CPU, Memória);

- 1.58. Deve permitir a criação de painéis personalizados para monitorar operações de segurança e rede;
- 1.59. Deve possuir relatório de uso de aplicações e mídias sociais;
- 1.60. Deve possuir relatório de prevenção de perda de dados (DLP);
- 1.61. Deve possuir relatório de VPN, Prevenção de Intrusão (IPS), análise de ameaças cibernéticas;
- 1.62. Deve possuir relatório diário resumido de eventos e incidentes de segurança;
- 1.63. Deve possuir um relatório de tráfego DNS e e-mail;
- 1.64. Deve possuir relatório das 10 principais aplicações utilizadas na rede;
- 1.65. Deve possuir relatório dos 10 principais sites web utilizados na rede;
- 1.66. Deve possibilitar a visibilidade da utilização do balanceamento inteligente de links (SD-WAN), mostrando informações de utilização das regras por aplicação, largura de banda e níveis de serviços dos links (latência, Jitter e descarte de pacotes);
- 1.67. Deve permitir a correlação de eventos, provendo painéis diversos, bem como possibilitar a criação de novas telas para visualizar os recursos de rede e segurança;

2. CARACTERÍSTICAS ESPECÍFICAS DE GERENCIAMENTO CENTRALIZADO DE LOGS E RELATORIA:

- 2.1. A solução deve suportar receber, no mínimo, 6 (seis) GB de logs diários;
- 2.2. Deve suportar o empilhamento de licenças, permitindo-se a soma de capacidade de logs diários.

ITEM 4 - Serviço de Implantação, Migração e Configuração.

1. O serviço de instalação e configuração dos Itens 1,2 e 3 deverão ser executados presencialmente na Sede Administrativa do TCERR, no Data Center da Diretoria de Tecnologia da Informação - DITIN, situado na Rua Prof. Agnelo Bittencourt, 126, Centro Boa Vista - RR;
2. A Contratada deverá implantar e configurar a solução, inclusive migrando todas as configurações existentes no firewall atual do TCERR.

ITEM 5 - Serviço de Treinamento de equipe técnica do Contratante.

1. A transferência de conhecimento técnico será feita através de treinamento hands-on referente aos Itens 1, 2 e 3, objeto deste Contrato e do Termo de Referência, abrangendo a administração e gerenciamento da solução, para até 5 (cinco) técnicos designados pela Contratante, com carga horária de no mínimo 16 horas.
2. O treinamento à equipe local do Tribunal será realizado na modalidade presencial, preferencialmente nos períodos das 08:00 às 12:00 e das 14:00 às 18:00, em dias úteis e em horário a ser definido pelo Tribunal;
3. A contratada deverá ministrar treinamento para até 5 de participantes da equipe técnica da Contratante;
4. O treinamento deverá abranger o repasse de informações e conhecimentos referentes à administração e gerenciamento da solução Itens (1,2 e 3), bem como o esclarecimento de dúvidas;
5. O treinamento deverá ser ministrado em língua portuguesa por profissional certificado pelo fabricante do produto ofertado.

ITEM 6 - Serviços Técnicos Especializados em Segurança da Informação (sob demanda)

1. Os serviços técnicos especializados (sob demanda) devem atender às seguintes especificações:
 - 1.1. Os Serviços Gerenciados de Segurança devem englobar a prestação de serviços técnicos especializados em segurança da informação, sob demanda, em um total de 120 (cento e vinte) horas;
 - 1.2. Os serviços devem ser baseados em horas de serviço, envolvendo atividades a serem demandadas por meio de celebração prévia de ordens de serviço, de comum acordo entre o Contratante e a Contratada, cujo pagamento será efetivado após a entrega dos serviços e relatório de execução;
 - 1.3. Execução de serviços no escopo da solução de Serviços Gerenciados de Segurança, limitando-se, exclusivamente, aos seguintes casos:

- 1.3.1. Elaboração de pareceres em segurança da informação;
- 1.3.2. Análise e suporte de planos de melhoria de infraestrutura de segurança do TCE/RR;
- 1.3.3. Suporte a mudanças de arquitetura do ambiente computacional do TCE/RR;
- 1.3.4. Movimentação de equipamentos (moving);
- 1.3.5. Avaliação de vulnerabilidades de ativos de rede do TCE/RR fora do escopo do projeto;
- 1.3.6. Apoio na definição e implementação de mecanismos futuros de monitoramento e recursos de segurança;
- 1.3.7. Desenvolvimento e implantação de boletins de segurança não revistos;
- 1.3.8. Desenvolvimento e implantação de indicadores de segurança não previstos;
- 1.3.9. Transferência de conhecimento por meio de workshops para questões de segurança.
- 1.4. Execução de serviços por meio de Ordem de Serviço Técnico Especializado, previamente definida, documentada, protocolada e aprovada, em comum acordo entre a Contratante e a Contratada, sobretudo quanto ao tempo necessário de atendimento;
- 1.5. Execução de serviço por profissional com perfil adequado, que deve ser demonstrado com certificação CISSP e experiência comprovada de 5 anos na área de segurança da informação;
- 1.6. Apresentação de relatório de execução pela Contratada, com justificativas plausíveis e aceitas pela Contratante, quando solicitada prorrogação do prazo de execução de uma Ordem de Serviço Técnico Especializado;
- 1.7. Conclusão e validação de uma Ordem de Serviço Técnico Especializado somente após entrega da documentação com relatório das atividades desenvolvidas.

GRUPO 02			
7	Serviço de SOC 24x7 com SIEM, período de 36 meses	Serv./mês	36
8	Serviços Técnicos Especializados (SOC) (sob demanda) pelo período de 36 meses.	UST	1080

ITEM 7 - Serviço de SOC 24x7 com SIEM, período de 36 meses

1. Escopo dos serviços gerenciados de segurança da informação

1.1. A monitoração remota, contínua e ininterrupta (24×7×365) deverá atender ao seguinte escopo técnico:

1.1.1. A solução a ser empregada deve estar corretamente dimensionada e licenciada para suportar os ativos elencados abaixo, a serem monitorados, com capacidade mínima estimada de processamento de pelo menos 1 mil (um mil) eventos por segundo (EPS), garantindo desempenho compatível com o volume e a criticidade do ambiente do TRIBUNAL DE CONTAS DE RORAIMA:

Ambiente Tecnológico	Marca
Solução de Next Generation Firewall/IPS/WAF	2 (Um ativo e outro passivo)
	1 WAF
Solução Segurança Estações (EDR)	1 Servidor
Solução AD	2
Servidores de Banco de Dados	3 Postgres
	1 Mysql
	150 - Linux

Sistemas Operacionais Ambiente Tecnológico	Marca
	10-Windows
Ativos de Rede	8 (Switches de Borda + Anel)

1.1.2. Caso os quantitativos da tabela acima ultrapassem 1 mil (um mil) eventos por segundo (EPS), o CONTRATANTE deverá readequar junto à CONTRATADA, informando quais itens irão ser monitorados.

1.2. O serviço de monitoração deverá contemplar os seguintes processos operacionais:

1.2.1. Centralização e gestão das soluções:

1.2.1.1. A CONTRATADA atuará de forma contínua e proativa na prestação de serviços de SOC (Security Operations Center), com foco nas atividades de monitoramento, detecção, triagem e resposta a incidentes de segurança da informação, utilizando principalmente as plataformas de SIEM contratadas. A equipe técnica da CONTRATADA será responsável por analisar os alertas gerados, qualificar os eventos, iniciar procedimentos automatizados quando aplicável, e acionar as equipes responsáveis inclusive os fornecedores de soluções específicas já contratados pelo TRIBUNAL DE CONTAS DE RORAIMA sempre que identificada a necessidade de atuação externa. Nessas situações, a CONTRATANTE atuará como ponto focal de acionamento técnico, abrindo e acompanhando os chamados junto aos canais de suporte dos fornecedores, encaminhando logs, evidências e informações relevantes, a fim de manter às equipes envolvidas alinhadas sobre o progresso e a previsão de resolução. Importante destacar que a CONTRATADA não executará intervenções diretas nas soluções de terceiros, tampouco será responsável pela resolução dos problemas, mas sim por sua correta identificação, classificação, documentação e encaminhamento.

1.2.1.2. A CONTRATADA poderá atuar como ponto focal técnico-operacional em casos de incidente de segurança, desde que autorizado pelo CONTRATANTE, na gestão e acionamento das empresas fornecedoras das soluções de segurança da informação atualmente em uso no TRIBUNAL DE CONTAS DE RORAIMA, sendo acompanhado pelo equipe técnica do TCERR. Essa atuação visa assegurar agilidade, rastreabilidade e centralização na comunicação com os diversos prestadores de serviços relacionados ao ambiente de segurança cibernética da Instituição.

1.2.1.3 O papel da CONTRATADA é de apoio técnico e coordenação dos acionamentos, não sendo de sua responsabilidade executar as ações corretivas diretamente nas soluções administradas, tampouco intervir nas tratativas internas dos fornecedores com os fabricantes.

1.2.1.4. A responsabilidade pela correção dos problemas, mitigação dos incidentes e cumprimento dos níveis de serviço (SLAs) estabelecidos com o TRIBUNAL DE CONTAS DE RORAIMA será exclusiva dos fornecedores responsáveis por cada solução.

1.2.1.5. A CONTRATADA não poderá ser responsabilizada pelo eventual não cumprimento dos SLAs atribuídos aos fornecedores das soluções, desde que tenha realizado, de forma tempestiva e documentada, o acionamento e o devido acompanhamento das ocorrências.

1.2.1.6. A CONTRATADA deverá apresentar relatórios periódicos contendo o histórico dos acionamentos, os tempos de resposta dos fornecedores, os encaminhamentos realizados e quaisquer riscos identificados, permitindo ao TRIBUNAL DE CONTAS DE RORAIMA a avaliação contínua da qualidade dos serviços prestados por terceiros.

1.3. Triagem de Incidentes:

1.3.1. A CONTRATADA deverá realizar triagem inicial dos alertas gerados durante o processo de monitoração, consolidando aqueles que apresentem características similares como ataques direcionados ao mesmo ativo, origens de ataque idênticas (mesmo IP), múltiplas tentativas de login malsucedidas, entre outros padrões.

1.3.2. Após a triagem, os eventos deverão ser avaliados individualmente, com o objetivo de identificar possíveis falsos-positivos e validar a veracidade dos incidentes. Essa etapa deverá incluir testes, análises contextuais e correlação com outras fontes para confirmar a ocorrência e a natureza da ameaça.

1.4. Resposta a incidentes:

1.4.1. Em caso de identificação de um potencial incidente de segurança, a CONTRATADA deverá registrar a ocorrência tanto em seu próprio sistema de gerenciamento de chamados, garantindo o devido

acompanhamento do evento. O chamado deverá conter, obrigatoriamente, informações como: origem e tipo do ataque, data e hora da detecção, registros de log, causa provável do incidente e os procedimentos adotados na resposta, de forma a viabilizar a execução das medidas corretivas necessárias, seja por sua equipe, seja em conjunto com a equipe técnica do TRIBUNAL DE CONTAS DE RORAIMA, quando aplicável.

1.4.2. Serão considerados incidentes de segurança todos os eventos adversos relacionados aos ativos monitorados que possam afetar a confidencialidade, a integridade ou a disponibilidade das informações ou serviços do TRIBUNAL DE CONTAS DE RORAIMA. Entre eles, incluem-se, a título exemplificativo: acessos não autorizados, instalação de softwares maliciosos, ataques de negação de serviço (DoS/DDoS), tentativas de intrusão por força bruta, entre outros.

1.4.3. Concluído o tratamento do incidente, a CONTRATADA deverá elaborar e encaminhar um relatório técnico à equipe do TRIBUNAL DE CONTAS DE RORAIMA, contendo o histórico do evento, as ações corretivas realizadas e recomendações de melhorias que possam prevenir novas ocorrências ou mitigar impactos em situações similares futuras.

1.5. Problemas

1.5.1. A equipe da CONTRATADA deverá registrar chamados de problema em seu próprio sistema, sempre que identificadas ocorrências no serviço de monitoração que demandem investigação aprofundada. Esses chamados deverão ter como objetivo a identificação da causa raiz das falhas ou anomalias observadas. Após a análise, a CONTRATADA deverá executar as ações corretivas necessárias para a resolução dos problemas detectados, atuando de forma autônoma ou, quando aplicável, em conjunto com a equipe técnica do TRIBUNAL DE CONTAS DE RORAIMA, assegurando a restauração plena do serviço e a mitigação de riscos associados.

1.6. Armazenamento de logs (registros) de auditoria

1.6.1. Caso o CONTRATANTE entenda que as informações registradas nos arquivos de logs são insuficientes para fins de auditoria, investigação ou conformidade, poderá solicitar à CONTRATADA ajustes ou reconfigurações na captura e armazenamento desses registros, de forma a garantir a completude e a qualidade dos dados.

1.6.2. Os logs gerados durante a prestação dos serviços deverão ser mantidos por um período de até 2 (dois) meses de forma indexada e por um período de 12 (doze) meses em forma de backup, podendo ser restaurados quando solicitado. 36Ao término do contrato, a CONTRATADA deverá repassar integralmente esses registros ao TRIBUNAL DE CONTAS DE RORAIMA, em formato digital apropriado, e comprovar a eliminação definitiva de quaisquer cópias sob sua guarda, observando as boas práticas de segurança da informação e os requisitos legais aplicáveis.

1.6.3. O período mínimo de retenção online dos registros deverá ser de 2 (dois) meses, sendo permitido que os meses restantes sejam armazenados em meio offline em até 12 (doze) meses, desde que o acesso a essas informações possa ser realizado de forma imediata sempre que solicitado.

1.7. Ferramentas e Soluções Tecnológicas Integradas à Monitoração de Segurança.

1.7.1. Toda a infraestrutura tecnológica necessária à prestação dos serviços incluindo softwares, hardwares e respectivos licenciamentos deverá ser fornecida integralmente pela CONTRATADA, sem ônus adicional para o TRIBUNAL DE CONTAS DE RORAIMA durante toda a vigência contratual. Essa infraestrutura poderá estar instalada em ambiente próprio da CONTRATADA, o qual poderá ser composto por recursos localizados em suas dependências físicas, hospedados em nuvem de terceiros por ela contratada, ou hospedada em nuvem do próprio fabricante da solução, desde que garantidas a segurança, a disponibilidade e a performance exigidas para a operação dos serviços de monitoração, gestão e administração remota da segurança da informação.

1.7.2. A CONTRATADA será responsável por manter em dia as licenças/subscrições exigidas para o funcionamento dos componentes de hardware e/ou software fornecidos, incluindo o relacionamento com os respectivos fabricantes. A equipe técnica do TRIBUNAL DE CONTAS DE RORAIMA poderá, a qualquer momento durante a execução do contrato, solicitar documentação comprobatória da regularidade dessas licenças.

1.7.3. A CONTRATADA assumirá integral responsabilidade pela execução das manutenções preventivas e corretivas dos equipamentos por ela fornecidos, sem qualquer ônus adicional ao TRIBUNAL DE CONTAS DE RORAIMA.

1.7.4. A CONTRATADA deverá garantir a total disponibilidade, funcionamento contínuo e desempenho adequado da solução tecnológica ofertada tanto em hardware quanto em software durante todo o período de vigência do contrato.

1.7.5. Os recursos destinados à plena utilização e atendimento aos serviços requeridos pela CONTRATANTE deverão ser e estar hospedados em infraestrutura de DATACENTER que possua certificação Uptime Tier III ou compatível, a ser disponibilizada exclusivamente pela LICITANTE vencedora e por conseguida CONTRATADA. 46Todas as exigências mínimas contidas nos itens abaixo são indispensáveis e o não atendimento a qualquer um desses itens é motivo suficiente para a imediata desclassificação da LICITANTE.

1.7.6. O serviço deve contemplar dois ou mais Centros de Operações de Segurança (SOC), operando em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, todos os dias do ano);

1.7.7. O Centro de Operações de Segurança (SOC) deverá estar localizado em território nacional e devidamente operacional na data da assinatura do Contrato, sendo vedada sua implantação ou ativação posterior ao início da vigência contratual.

1.7.8. O TRIBUNAL DE CONTAS DE RORAIMA poderá realizar vistorias técnicas a qualquer tempo durante a vigência contratual, com o objetivo de verificar o cumprimento das exigências estabelecidas neste Termo de Referência, sendo de responsabilidade da CONTRATADA garantir o pleno atendimento às condições pactuadas.

1.7.9. A CONTRATADA deve prover níveis de segurança elevados, utilizando no SOC ferramentas para garantir a segurança dos dados manipulados, contemplando, no mínimo, os seguintes controles de segurança física e lógica:

1.7.9.1. Controle de acesso físico ao SOC, com a utilização de pelo menos 02 (dois) mecanismos de autenticação, sendo, no mínimo, um deles por biometria;

1.7.9.2. Monitoramento por sistema interno de TV (CFTV), armazenando as imagens dos últimos 30 (trinta) dias;

1.7.9.3. Todos os funcionários da CONTRATADA envolvidos na operação ou que possuam acesso às informações do CONTRATANTE devem assinar termo de responsabilidade e sigilo;

1.7.9.4. A CONTRATADA deve disponibilizar toda a infraestrutura necessária para o monitoramento dos alertas de segurança realizado por seus analistas, em regime 24 X 7 (24 horas por dia, 7 dias da semana);

1.7.9.5. A CONTRATADA deve realizar as ações necessárias para identificação de incidentes de segurança por meio dos dados e alertas monitorados na Solução Integrada de SOC, que podem comprometer a segurança dos serviços e ativos do CONTRATANTE. A CONTRATADA deve analisar eventos detectados, classificar e categorizar conforme definição do CONTRATANTE. Identificar, registrar, escalar e notificar os incidentes de segurança ao CONTRATANTE para tratamento;

1.7.9.6. A CONTRATADA é responsável pelas atividades de camada 1 do SOC, que para o modelo definido corresponde minimamente às atividades relacionadas abaixo:

1.7.9.6.1. Definição de linha base (baseline) de forma a entender o comportamento normal do ambiente monitorado, ajustando métricas eliminando de detecção, com o objetivo de reduzir o número de falsos positivos e aumentar a precisão da detecção.

1.7.9.6.2. Monitoração de alertas de segurança, onde o analista deve decidir se uma análise é necessária. A detecção consiste em avaliar os alertas de segurança dos sensores buscando indicadores de comportamentos maliciosos que ultrapassem os limites estabelecidos no baseline. A lógica de detecção deve ser ajustada e desenvolvida, podendo passar a utilizar múltiplos eventos e diferentes fontes de dados. Os alertas devem indicar minimamente:

1.7.9.6.2.1. Ataques de força bruta com e sem sucesso;

1.7.9.6.2.2. Falhas de autenticação que indiquem suspeita de roubo de identidade;

1.7.9.6.2.3. Infecção de equipamentos por vírus;

1.7.9.6.2.4. Comprometimento de ativos da rede;

1.7.9.6.2.5. Realização de ações suspeitas por parte de usuários privilegiados;

1.7.9.6.2.6. Alertas de operação de serviços, como interrupções e falhas;

1.7.9.6.2.7. Ataques de negação de serviço;

1.7.9.6.2.8. Ataques comuns em aplicações WEB, como XSS e SQL injection;

1.7.9.6.2.9. Atividades de botnets;

1.7.9.6.2.10. Exploração de vulnerabilidades;

1.7.9.6.3. Detecção por análise de logs, onde o analista realiza pesquisas, revisões e análises estatísticas no histórico de log armazenado na Solução Integrada de SOC, com o objetivo de identificar comportamentos e evidências que indiquem atividades maliciosas ou novas ameaças.

1.7.9.6.4. Análise de eventos, onde o analista deve pesquisar informações adicionais que podem estar relacionadas ao evento em análise, que forneçam algum valor investigativo para identificar comportamentos anômalos ou maliciosos. A análise realizada nessa etapa é preliminar, tendo o objetivo de confirmar a ocorrência de um evento de segurança, eliminando falsos positivos confirmados. O resultado da análise pode ser uma das seguintes categorias:

1.7.9.6.4.1. Evento confirmado: os sensores detectaram corretamente uma ameaça válida. Os incidentes confirmados devem ser escalados para a etapa de mitigação da gestão de incidentes;

1.7.9.6.4.2. Falso positivo: ocorre quando o sistema detecta incorretamente uma ameaça ou não existe risco no evento detectado, sendo eventos alertados como maliciosos, mas não são;

1.7.9.6.4.3. Eventos autorizados: são ameaças detectadas corretamente, mas que são aprovadas pela política de segurança, como por exemplo, a análise de vulnerabilidades;

1.7.9.6.4.4. Indeterminado: quando não existe evidência suficiente para confirmar o evento de segurança;

1.7.9.6.5. Registro de análise, todo evento detectado que for selecionado para análise, deve ser registrado no Sistema de Ticket ofertado, incluindo as atividades de investigação. O resultado da análise pode ser a definição de um falso positivo, encerrando o tíquete, ou a confirmação de um incidente de segurança, escalando o tíquete para tratamento. O tíquete deve conter as seguintes informações:

1.7.9.6.5.1. Identificador do ticket;

1.7.9.6.5.2. Sensor que detectou o evento;

1.7.9.6.5.3. Identificador do evento gerado no sensor;

1.7.9.6.5.4. Limiar de detecção utilizado para enviar o evento para análise;

1.7.9.6.5.5. Log do evento detectado;

1.7.9.6.5.6. Origem e categoria do ataque;

1.7.9.6.5.7. Data e hora;

1.7.9.6.6. Triagem e Categorização de eventos, os tíquetes registrados devem ser priorizados por categorias, unificando os eventos potenciais de incidentes com as características em comum, que podem receber tratamento padronizado. Os eventos confirmados, classificados como incidente, devem ter seu tíquete escalado para os analistas do CONTRATANTE;

1.7.10. Elaboração de relatórios. A CONTRATADA deverá disponibilizar relatórios em formato PDF, referentes aos indicadores monitorados com periodicidade mínima mensal, ou sob demanda, podendo incluir:

1.7.10.1. Classificação dos eventos de segurança;

1.7.10.2. Total de eventos avaliados;

1.7.10.3. Total de eventos escalados;

1.7.10.4. TOP aplicações mais impactadas, TOP origens dos eventos de segurança;

1.7.10.5. TOP endereços de destino das ameaças;

1.7.10.6. URLs e suas categorias;

1.7.10.7. TOP atacantes, vulnerabilidades, ameaças, alarmes, violações de auditoria;

1.7.10.8. Principais tipos de ataques;

1.7.10.9. Novas informações de inteligência configuradas na ferramenta: como as novas regras de monitoramento, dashboards, assinaturas instaladas, etc;

1.7.11. O Sistema de Ticket ofertado deverá ser utilizado para registrar e escalar eventos de segurança, de modo a permitir o registro, envio de notificações e alertas entre as equipes do CONTRATANTE e da própria CONTRATADA;

1.7.12. O CONTRATANTE é responsável por avaliar os incidentes escalados após o processo de triagem inicial. Caso o incidente seja confirmado, o CONTRATANTE executará os seus processos e procedimentos internos para executar as medidas de contenção e correção, incluindo configurações nos sensores de segurança ou outros ativos. O CONTRATANTE registrará as ações realizadas no tíquete correspondente ao incidente, permitindo que a CONTRATADA esteja ciente do fechamento do mesmo;

1.7.13. Os analistas do CONTRATANTE devem poder contatar os analistas da CONTRATADA, por telefone ou via Sistema de Ticket, para consulta de informações em caso de qualquer dúvida sobre os eventos escalados e demais procedimentos para tratamento dos incidentes. As solicitações e respostas de informações adicionais sobre os incidentes, como logs e evidências, devem ser anexadas ao tíquete registrado na ferramenta;

1.7.14. O CONTRATANTE pode solicitar, a qualquer momento, a customização dos indicadores e informações sobre incidentes e eventos apresentados nos relatórios. A CONTRATADA deve avaliar os requisitos técnicos necessários e operacionalizar. As solicitações devem ser registradas e realizadas por meio dos canais de suporte da CONTRATADA;

1.7.15. A CONTRATADA deve prover informação específica sobre ameaças, gerada através de um processo (com coleta, validação, correlação, avaliação e interpretação de conhecimento baseado em evidências), que colocam em perigo ativos de informação ou de tecnologia do CONTRATANTE. Tal inteligência pode ser usada para embasar decisões sobre a resposta a tal ameaça ou risco, permitindo melhorar as táticas de detecção de ataques e configuração dos sensores de segurança. O processo deve resultar ainda em conhecimento utilizado para criação de novos indicadores e auxiliar na detecção de ataques futuros, possibilitando a identificação de ameaças específicas ao ambiente do CONTRATANTE;

1.7.16. Os serviços relacionados à coleta e correlação de logs deverão contemplar as características descritas a seguir:

1.7.16.1. A CONTRATADA deverá prover uma solução de SIEM (Security Information and Event Management), devidamente configurada e ajustada às necessidades operacionais e de segurança do TRIBUNAL DE CONTAS DE RORAIMA.

1.7.16.2. Compete à CONTRATADA a implementação das regras, políticas de segurança, filtros e configurações específicas na solução de SIEM, de acordo com os requisitos técnicos do ambiente do TRIBUNAL DE CONTAS DE RORAIMA e com as melhores práticas de mercado.

1.7.16.3. A solução deverá ser capaz de realizar a coleta, análise e correlação de logs e eventos provenientes de diferentes fontes, possibilitando a detecção de atividades anômalas, padrões de ataque e riscos à integridade do ambiente monitorado.

1.7.16.4. A responsabilidade pelo envio dos logs dos ativos (como switches, roteadores, servidores, entre outros) será do TRIBUNAL DE CONTAS DE RORAIMA, por meio da configuração de seus próprios equipamentos. Por sua vez, a CONTRATADA será responsável por toda a configuração e gestão da solução de SIEM, garantindo o correto recebimento e tratamento dos dados enviados.

1.7.16.5. A solução de SIEM deverá ser capaz de gerar chamados automaticamente no portal de atendimento da CONTRATADA sempre que identificar indícios de incidentes de segurança ou indisponibilidade. Idealmente, esses mesmos chamados também deverão ser abertos automaticamente, ou por meio de integração, na ferramenta de gestão de incidentes e requisições utilizada pelo TRIBUNAL DE CONTAS DE RORAIMA.

1.7.17. Caberá à CONTRATADA executar de forma integral todas as atividades relacionadas à monitoração, operação, administração remota e manutenção da solução de SIEM, incluindo, mas não se limitando a:

1.7.17.1. Elaboração e manutenção de regras de correlação de eventos, assegurando que todos os ativos monitorados estejam contemplados, sem a imposição de limites mínimos por ativo;

1.7.17.2. Execução de todas as configurações necessárias à operação e à adaptação da solução ao ambiente do TRIBUNAL DE CONTAS DE RORAIMA;

1.7.17.3. Interação direta com o fabricante da solução de SIEM para resolução de questões técnicas, aplicação de boas práticas ou suporte de terceiro nível;

1.7.17.4. Realização rotineira de cópias de segurança (backup) e restauração (restore) dos dados e configurações da plataforma;

1.7.17.5. Atuação na identificação e correção de falhas e anomalias relacionadas ao funcionamento da solução;

1.7.17.6. Prestação de suporte técnico especializado, de acordo com os níveis de serviço acordados;

1.7.17.7. Instalação e ativação de serviços e funcionalidades previstos no escopo contratual, conforme necessidade do TRIBUNAL DE CONTAS DE RORAIMA;

1.7.17.8. Atualização da solução, incluindo aplicação de patches, correções e novas versões, conforme as recomendações e diretrizes do fabricante.

1.7.17.9. Durante a fase de implantação, a CONTRATADA realizará a configuração e o ajuste fino dos serviços. Fica estabelecido um período de Operação Assistida, com duração de 120 (cento e vinte) dias, a contar da assinatura do contrato. Este período é destinado ao amadurecimento da operação, à calibração das regras de detecção para o ambiente específico do TRIBUNAL DE CONTAS DE RORAIMA e à estabilização do baseline de comportamento, não havendo, portanto, a aplicação de Acordos de Nível de Serviço (SLA) durante esta fase. O processo de implantação abrangerá, no mínimo, as seguintes macrofases, que culminaram no início do período de Operação Assistida:

1.7.17.9.1. Implantação e Configuração da Solução:

Instalação e configuração de todos os componentes da solução de SOC (Security Operations Center) ofertada;

1.7.17.9.2. Integração de Fontes de Log:

Integração das fontes de dados e logs do ambiente do TRIBUNAL DE CONTAS DE RORAIMA à plataforma de SIEM, a ser realizada em conjunto com a equipe técnica da CONTRATANTE;

1.7.17.9.3. Definição e Ativação das Regras de Correlação:

Apresentação, para validação e aprovação formal do TRIBUNAL DE CONTAS DE RORAIMA, de um conjunto inicial de, no mínimo, 30 regras de correlação, seguido de sua ativação na plataforma.

1.7.17.9.4. Operacionalização da Gestão de Incidentes:

Configuração e ativação da plataforma de gestão de incidentes para garantir o correto registro e escalonamento dos eventos de segurança identificados;

1.7.18. O TRIBUNAL DE CONTAS DE RORAIMA poderá, a qualquer tempo, solicitar ajustes ou modificações nas regras de correlação de eventos, de modo a garantir a aderência da solução às suas necessidades específicas e ao seu contexto operacional.

1.7.19. Toda nova regra a ser implementada pela CONTRATADA deverá ser devidamente documentada. Sempre que solicitado, essa documentação poderá ser submetida ao TRIBUNAL DE CONTAS DE RORAIMA para validação prévia, como forma de garantir transparência e rastreabilidade na evolução da configuração da solução.

1.8. A solução de SIEM fornecida pela CONTRATADA deverá atender, no mínimo, às seguintes características técnicas e funcionalidades:

1.8.1. Realizar a coleta e correlação de logs dos diversos componentes da infraestrutura tecnológica do TRIBUNAL DE CONTAS DE RORAIMA, incluindo ativos de rede (roteadores, switches, etc.), dispositivos de segurança (como firewalls e sistemas de prevenção de intrusão IPS), sistemas operacionais de servidores e aplicações corporativas;

1.8.2. Armazenar os eventos coletados em formato bruto (raw data), garantindo sua integridade e confidencialidade, com vistas à utilização em auditorias e análises periciais, quando necessário;

1.8.3. Classificar automaticamente os eventos com base no nível de risco, considerando uma pré-classificação da criticidade dos ativos monitorados no ambiente institucional;

1.8.4. Executar a análise e correlação de logs de forma automatizada, utilizando regras definidas e ajustáveis, capazes de identificar comportamentos anômalos, padrões de ataque e situações que indiquem comprometimento de segurança, com geração de alertas contextualizados e priorização conforme o impacto potencial.

1.8.5. O sistema de correlação de eventos de segurança deverá ser capaz de identificar alterações comportamentais significativas com base em dados históricos, como por exemplo a detecção de tráfego anômalo;

1.8.6. A arquitetura da solução deverá permitir a instalação de coletores locais no ambiente do TRIBUNAL DE CONTAS DE RORAIMA, com capacidade de interpretar (parsear) os dados recebidos e realizar compressão eficiente para transmissão e armazenamento;

1.8.7. Quando necessário o uso de agentes de coleta, estes deverão ser oficialmente certificados pelo fabricante e compatíveis com as seguintes plataformas: Windows Server 2022 ou superior, Linux CentOS versão 5.1 ou superior, Linux Ubuntu versão 9 ou superior, Red Hat 7 ou superior e Debian 11 ou superior;

1.8.8. A solução deverá suportar nativamente a coleta de logs das seguintes fontes e APIs, sem necessidade de customização: Windows Event Remote Collection (sem uso de WMI), Nessus API, Nexpose API e Qualys Scanner API;

1.8.9. Os agentes de coleta deverão possibilitar o monitoramento de integridade de arquivos, emitindo alertas para eventos como criação, alteração, exclusão ou leitura de arquivos sensíveis;

1.8.10. Os agentes deverão ainda suportar a coleta de logs via protocolo Syslog a partir de outras plataformas, possibilitando integração ampla com diferentes ativos da infraestrutura;

1.8.11. A solução deverá ser capaz de distinguir logs provenientes de servidores intermediários (relay logs), permitindo a correlação individualizada por fonte original, mesmo quando repassados por servidores Syslog;

1.8.12. Deverá ser disponibilizado um mecanismo de monitoramento da saúde dos agentes, com geração de alertas em caso de falhas, paradas ou mau funcionamento;

1.8.13. A solução deverá operar preferencialmente sem a necessidade de instalação de agentes, exceto em casos em que os dispositivos não disponibilizam logs via protocolo padrão (Syslog);

1.8.14. A plataforma deverá realizar a correlação dos eventos e geração de alertas em tempo real, com mínima latência entre a ocorrência do evento e sua identificação;

1.8.15. A solução deverá permitir a correlação de diferentes tipos de dados, incluindo logs de segurança, desempenho, disponibilidade e alterações nos sistemas monitorados;

1.8.16. A ferramenta deverá disponibilizar no mínimo 150 regras de correlação embarcadas, permitindo ainda a criação e customização ilimitada de novas regras, conforme necessidades específicas do TRIBUNAL DE CONTAS DE RORAIMA;

1.9. A geração de alertas deverá contemplar, pelo menos, os seguintes cenários de segurança (sem prejuízo de outros casos relevantes):

1.9.1. Análise de comportamento com base em estatísticas (Statistical Behavioral Analysis);

1.9.2. Detecção de varreduras de rede (host/port scans), tentativas negadas, ou variações abruptas de tráfego por origem/destino;

1.9.3. Ataques de força bruta, bem-sucedidos ou não;

1.9.4. Indícios de infecção por vírus ou ransomware;

1.9.5. Tentativas de invasão ou comprometimento de ativos da rede;

1.9.6. Anomalias de autenticação, como excesso de falhas, acessos fora do expediente, logins a partir de IPs incomuns;

1.9.7. Ações suspeitas praticadas por usuários com privilégios elevados;

1.9.8. Identificação de padrões incomuns, incluindo logs fora do comportamento normal conhecido;

1.9.9. Detecção de autenticações simultâneas ou incompatíveis geograficamente com as mesmas credenciais (indicando possível roubo de identidade);

1.9.10. Tentativas de bloqueio de contas e varredura de senhas (password scans);

1.9.11. Identificação de ataques a aplicações web, como XSS (Cross-Site Scripting) e SQL Injection;

1.9.12. Ataques de negação de serviço (DoS e DDoS);

1.9.13. Identificação automatizada e em tempo real da localização geográfica dos eventos (cidade, estado e país), não se limitando apenas aos endereços IP;

1.9.14. Detecção de botnets, worms, ataques DDoS e malwares do tipo zero-day, por meio da correlação de logs de DNS, DHCP, proxies web, tráfego de rede, entre outras fontes suportadas pela solução.

1.9.15. As regras de correlação devem permitir desde configurações básicas, como a detecção por limiares (thresholds), até regras mais avançadas que utilizam operadores lógicos comuns para combinar diferentes tipos de eventos. A solução deverá possibilitar, por exemplo:

1.9.15.1. Os thresholds podem ser estáticos ou dinâmicos;

1.9.15.2. Possibilitar a execução de scripts automáticos para serem executados em casos de incidentes;

1.9.15.3. Possibilitar a configuração de política de notificações (severidade do incidente, hora do dia e serviço);

1.9.15.4. A solução será integrada com a monitoração de capacidade e desempenho dos ativos gerenciados via SNMP.

1.9.15.5. A auto detecção deverá ser capaz de:

1.9.15.5.1. A solução deverá permitir a pesquisa de eventos de segurança com os seguintes recursos mínimos:

1.9.15.5.1.1. Funcionalidade de busca em tempo real, utilizando sintaxes intuitivas, como palavras-chave do tipo "Google-like" ou consultas estruturadas similares a SQL ("SQL-like queries");

1.9.15.5.2. Capacidade de transformar os resultados das pesquisas em relatórios ou widgets personalizados para visualização em dashboards.

1.9.15.6. Painel de controle (dashboard) integrado à solução deverá contemplar os seguintes requisitos:

1.9.15.6.1. Disponibilização de visão consolidada das principais métricas de segurança relacionadas aos ativos monitorados;

1.9.15.6.2. Suporte à customização dos dashboards, com inclusão de gráficos, indicadores, relatórios e métricas relevantes ao ambiente do TRIBUNAL DE CONTAS DE RORAIMA;

1.9.15.6.3. Capacidade de análise em tempo real dos eventos de segurança da informação;

1.9.15.6.4. Suporte à navegação interativa por meio de drill-down, permitindo ao usuário detalhar informações a partir de gráficos gerais até níveis mais específicos, conforme necessário;

1.9.15.6.5. A console de visualização e consulta de eventos deverá também permitir a classificação dos registros em, no mínimo, três categorias distintas:

1.9.15.6.5.1. Eventos de Auditoria: como logins, logouts, falhas de autenticação, alterações de permissões;

1.9.15.6.5.2. Eventos de Segurança: tais como tentativas de ataque, comprometimento de ativos, exfiltração de dados, fraudes e atividades maliciosas;

1.9.15.6.5.3. Eventos de Operação: incluindo falhas críticas, indisponibilidades, erros de rede ou mau funcionamento de componentes.

1.9.15.7. A administração da solução deverá ser realizada por meio de interface web segura, acessível via protocolo HTTPS, garantindo a proteção das credenciais e da sessão administrativa;

1.9.15.8. A ferramenta deverá também disponibilizar funcionalidades avançadas de relatórios, abrangendo:

1.9.15.8.1. Geração de relatórios em tempo real e históricos;

1.9.15.8.2. Criação de relatórios de conformidade, cobrindo ao menos um dos frameworks: SOX, PCI ou ISO;

1.9.15.8.3. Deverá permitir a geração de consultas e visualizações configuráveis por escopo e período de análise, que, mediante solicitação do TRIBUNAL DE CONTAS DE RORAIMA, sirvam como base e evidência para atender a auditorias e demandas de compliance específicas;

1.9.15.8.4. Agendamento de relatórios personalizados, com execução automatizada em qualquer horário ou intervalo definido, com possibilidade de envio dos resultados por e-mail;

1.9.15.8.5. Exportação dos relatórios nos formatos Excel, PDF e CSV;

1.9.15.8.6. Classificação de eventos de segurança por tipo (ex: ataques, varreduras, malware, comportamento suspeito);

1.9.15.8.7. Análise de eventos por direção do tráfego (interno, externo e local);

1.9.15.8.8. Identificação dos principais destinos de ameaças detectadas (top endereços IP de destino);

1.9.15.8.9. Mapeamento geográfico de origem dos alertas, incluindo países e cidades;

1.9.15.8.10. Geração de notificações emergenciais 24x7x365, com envio de detalhamento técnico (incluindo logs relevantes) para subsidiar ações imediatas de contenção e resposta a incidentes de

ITEM 8 - Serviços Técnicos Especializados (SOC) (sob demanda) pelo período de 36 meses.

1. Os serviços especializados a serem prestados compreendem, entre outras, as seguintes atividades:

- 1.1. Elaboração de documentação técnica e de usuário, conforme padrões estabelecidos pelo CONTRATANTE;
- 1.2. Transferência de conhecimento técnico relacionado às atividades implantação e manutenção de soluções tecnológicas;
- 1.3. Levantamento de informações junto aos usuários, com o objetivo de definição e elaboração de regras de negócio, políticas e diretrizes operacionais;
- 1.4. Correção e/ou apoio na resolução de problemas e defeitos em funcionalidades já existentes;
- 1.5. Execução de operação assistida dos ambientes entregues com as soluções contratadas;
- 1.6. Orientação sobre o uso correto dos softwares instalados, conforme boas práticas e recomendações dos fabricantes;
- 1.7. Apoio nas atividades de atualização, instalação e/ou reinstalação de versões e produtos, com foco na minimização de impactos operacionais;
- 1.8. Apoio na configuração e parametrização de sistemas em novos equipamentos;
- 1.9. Suporte no levantamento de informações que possibilitem a identificação de novas necessidades no ambiente do CONTRATANTE;
- 1.10. Diagnóstico do funcionamento das ferramentas instaladas, visando garantir a máxima utilização dos recursos disponíveis;
- 1.11. Identificação e proposição de melhorias relacionadas à performance, desempenho, disponibilidade, confiabilidade e tuning de ambientes;
- 1.12. Otimização da reinstalação e/ou adaptação de ferramentas em equipamentos distintos daqueles da instalação original;
- 1.13. Definição de metodologias, elaboração de relatórios e projetos, bem como acompanhamento da configuração e utilização de soluções de alta disponibilidade, com repasse das melhores práticas aos técnicos do CONTRATANTE;
- 1.14. Esclarecimento de dúvidas e orientação aos técnicos de TI do CONTRATANTE quanto à integração das soluções com as diversas plataformas do ambiente computacional;
- 1.15. Apoio no planejamento, execução e avaliação de mudanças no ambiente de TI;
- 1.16. Análise de patches, correções e novas versões de software, com recomendação sobre sua aplicação ou não;
- 1.17. Apoio no planejamento, execução e avaliação de atualizações de versões e aplicação de patches;
- 1.18. Apoio no planejamento, execução e avaliação da implantação ou atualização de aplicações no ambiente do CONTRATANTE.
- 1.19. A adoção do valor de referência único facilita à contabilização dos serviços, todavia, demanda a definição dos parâmetros relativos à ponderação aplicável ao dimensionamento do serviço. Nesse sentido, para efeito de cada projeto a ser contratado, serão adotados os seguintes pesos de complexidade:

Complexidade	Serviços	Peso UST
Baixa	Levantamento de informações junto aos usuários, objetivando a definição e elaboração de regras e políticas; corrigir ou apoiar em problemas e defeitos em funcionalidades já existentes e atividades similares.	1,0

Complexidade	Serviços	Peso UST
Intermediária	Elaboração de documentação técnica e de usuário; diagnosticar o bom funcionamento das ferramentas instaladas, garantindo a máxima utilização dos recursos oferecidos e atividades similares.	1,05
Alta	Transferência de conhecimentos relacionados ao desenvolvimento, implantação e manutenção no ambiente do CONTRATANTE Identificar e elaborar proposição de melhoria em performance, desempenho, tuning, disponibilidade e confiabilidade em ambientes; otimizar a reinstalação e/ou adaptação das ferramentas em outros equipamentos que não seja onde originalmente os sistema e produtos foram instalados; esclarecer dúvidas e orientar os técnicos de TI do CONTRATANTE, sobre integração das soluções, abrangendo as diversas plataformas existentes no ambiente computacional do CONTRATANTE; apoiar no planejamento, na execução e na avaliação das atualizações de versões, aplicação de patches da ferramenta e atividades similares.	1,10
Especialista	Definir metodologia, elaborar relatórios e projetos e acompanhar a configuração e utilização de solução de alta disponibilidade, repassando aos técnicos da TI do CONTRATANTE as melhores práticas para uso da solução, quanto à configuração e parametrização dos componentes e ferramentas utilizadas no CONTRATANTE; apoiar no planejamento, na execução e na avaliação das mudanças no ambiente; analisar patches, correções e novas versões e sugerir a aplicação ou não dos mesmos no ambiente; apoiar no planejamento, na execução e na avaliação de implantação de novas aplicações ou atualização de aplicações no ambiente e atividades similares.	1,15

1.20. Características da contratação dos serviços:

1.20.1. O objeto tem por escopo a prestação de serviços de natureza contínua, realizados sob demanda, voltados à execução de atividades técnicas especializadas em tecnologia da informação e comunicação (TIC). Esses serviços são considerados fundamentais para assegurar a continuidade e a efetividade dos objetivos estratégicos da CONTRATANTE, bem como dos serviços prestados aos seus clientes finais, em que a infraestrutura de TIC representa elemento crítico de suporte.

1.20.2. A execução dos serviços deverá ser pautada por:

1.20.2.1. Flexibilidade e agilidade no atendimento das demandas

1.20.2.2. Cumprimento das normas, políticas internas e boas práticas adotadas pela CONTRATANTE;

1.20.2.3. Compromisso com a transferência de conhecimento para a equipe técnica da CONTRATANTE;

1.20.2.4. Garantia de rastreabilidade das ações e entregas, com elaboração de documentação técnica correspondente.

Anexo II – Tabela de Correlação de Requisitos do Termo de Referência e Proposta Técnica (Ponto a Ponto)

Grupo 1 – Firewall

Item	Requisito do TR	Página/URL	Documentação do Fabricante	Atenderá Durante a Execução do Contrato	Observação
1	Itens do Anexo I				
2					
3					

Item	Requisito do TR	Página/URL	Documentação do Fabricante	Atenderá Durante a Execução do Contrato	Observação
4					

Grupo 2 – SOC (Security Operations Center)

Item	Requisito do TR	Página/Url	Documentação do Fabricante	Atenderá durante a Execução do Contrato	Observação
1	Itens do Anexo I				
2					
3					
4					

Explicação das colunas e recomendações para preenchimento

- **Item:** número sequencial do requisito, para referência rápida, seguindo a numeração do **Anexo I** deste Termo de Referência.
- **Requisito do TR:** descrição detalhada do requisito definido no Termo de Referência.
- **Página/URL:** indicar a página do documento fornecido que comprova o atendimento ao requisito.
- **Documentação do Fabricante:** indicar qual documento do fabricante está sendo apresentado como evidência (manual, certificado, especificação técnica, etc.).
- **Atenderá durante a Execução do Contrato:** O item não tem como comprovar antes da execução do serviço, neste caso o licitante poderá marcar com um "X" e não especificar as demais colunas.
- **Observação:**
 - Este campo deve ser preenchido pela empresa com informações adicionais que **comprovem e detalhem como o requisito está sendo atendido**.
 - Recomenda-se que a empresa organize essas informações em **uma planilha complementar**, relacionando cada item do TR à evidência apresentada, incluindo links, documentos anexos ou explicações detalhadas.
 - Pode-se incluir comentários sobre limitações, alternativas ou adaptações propostas.

ANEXO II – DO EDITAL

MODELO DE APRESENTAÇÃO DAS PROPOSTAS DE PREÇOS

REF: Licitação nº 022/2025- Pregão Eletrônico

Prezados Senhores,

Estamos cotando o **GRUPO DE ITENS**, a seguir relacionado, com vista ao seu fornecimento ao Tribunal de Contas do Estado de Roraima/Boa Vista/RR, de acordo com o disposto na Lei no. 14.133, de 01 de abril de 2021.

GRUPO 1 [FIREWALL]					
Item	Descrição dos Serviços	Unidade.	Quantidade	Valor Unitário R\$	Valor Total R\$

1	Serviço de Gerenciamento de Tecnologia de Segurança de Rede (UTM-NGFW) , garantia e suporte técnico pelo período de 60 meses , com disponibilidade de 2 equipamentos em regime de comodato	Serv./mês	60		
2	Serviço de Gerenciamento de Tecnologia de Segurança de Rede Aplicação WEB (WAF - Web Application Firewall) , garantia e suporte técnico pelo período de 60 meses , com disponibilidade de equipamentos em regime de comodato.	Serv./mês	60		
3	Solução de Relatoria , garantia e suporte técnico pelo período de 60 meses .	Serv./mês	60		
4	Serviço de Implantação, Migração e Configuração.	Serv	1		
5	Serviço de Treinamento de equipe técnica do Contratante.	Serv	1		
6	Serviços Técnicos Especializados em Segurança da Informação (sob demanda)	UST	120		
Preços Globais do GRUPO 01 R\$					

Tabela 1 - Valor estimado de Firewall Grupo 1

Valor numérico e por extenso: Valor Total da Proposta R\$:

Validade da Proposta: _____ dias (MÍNIMO DE 60 DIAS CORRIDOS)

Prazo de Pagamento: até o **10 dias úteis** após o atesto da nota fiscal no TCE/RR.

Empresa: _____

Endereço: _____ Bairro: _____

CEP: _____ Fone/Fax: _____ / _____

Email: _____

Inscrição Estadual: _____ N°. Conta

Corrente: _____ N°. Agência: _____ Banco: _____

Declaração: Estão incluídos todos os encargos trabalhistas, previdenciários, fiscais, comerciais, de transporte, entrega e outros de qualquer natureza que se fizerem indispensáveis à perfeita contratação do objeto da licitação.

(*) Os valores máximos individuais e totais dos itens estão descritos no Anexo I Do Edital.

Boa Vista, _____ de _____ de 2026.

Assinatura e Identificação do Representante

REF: Licitação nº 022/2025- Pregão Eletrônico

Prezados Senhores,

Estamos cotando o **GRUPO DE ITENS**, a seguir relacionado, com vista ao seu fornecimento ao Tribunal de Contas do Estado de Roraima/Boa Vista/RR, de acordo com o disposto na Lei no. 14.133, de 01 de abril de 2021.

GRUPO 2
[SOC]

Item	Descrição dos Serviços	Unidade.	Quantidade	Valor Unitário R\$	Valor Total R\$
7	Serviço de SOC 24x7 com SIEM, período de 36 meses	Serv./mês	36		
8	Serviços Técnicos Especializados (SOC) (sob demanda) pelo período de 36 meses.	UST	1080		
Preços Globais do GRUPO 02 R\$					

Valor numérico e por extenso: Valor Total da Proposta R\$:

Validade da Proposta: _____ dias (MÍNIMO DE 60 DIAS CORRIDOS)

Prazo de Pagamento: até o 10 dias úteis após o atesto da nota fiscal no TCE/RR.

Empresa: _____

Endereço: _____ Bairro: _____

CEP: _____ Fone/Fax: _____ / _____

Email: _____

Inscrição Estadual: _____ Nº. Conta Corrente: _____ Nº. Agência: _____ Banco: _____

Declaração: Estão incluídos todos os encargos trabalhistas, previdenciários, fiscais, comerciais, de transporte, entrega e outros de qualquer natureza que se fizerem indispensáveis à perfeita contratação do objeto da licitação.

(*) Os valores máximos individuais e totais dos itens estão descritos no Anexo I Do Edital.

Boa Vista, _____ de _____ de 2026.

Assinatura e Identificação do Representante

ANEXO II - A – DO EDITAL

TABELA DE CORRELAÇÃO DE REQUISITOS DO TERMO DE REFERÊNCIA E PROPOSTA TÉCNICA (PONTO A PONTO).

Grupo 1 – Firewall

Item	Requisito do TR	Página/URL	Documentação do Fabricante	Atenderá Durante a Execução do Contrato	Observação
1	Itens do Anexo I				
2					
3					
4					

Grupo 2 – SOC (Security Operations Center)

Item	Requisito do TR	Página/Url	Documentação do Fabricante	Atenderá durante a Execução do Contrato	Observação
1	Itens do Anexo I				
2					
3					

Explicação das colunas e recomendações para preenchimento

- **Item:** número sequencial do requisito, para referência rápida, seguindo a numeração do Anexo I deste Termo de Referência.
- **Requisito do TR:** descrição detalhada do requisito definido no Termo de Referência.
- **Página/URL:** indicar a página do documento fornecido que comprova o atendimento ao requisito.
- **Documentação do Fabricante:** indicar qual documento do fabricante está sendo apresentado como evidência (manual, certificado, especificação técnica, etc.).
- Atenderá durante a Execução do Contrato: O item não tem como comprovar antes da execução do serviço, neste caso o licitante poderá marcar com um "X" e não especificar as demais colunas.
- **Observação:**
 - Este campo deve ser preenchido pela empresa com informações adicionais que **comprovem e detalhem como o requisito está sendo atendido**.
 - Recomenda-se que a empresa organize essas informações em **uma planilha complementar**, relacionando cada item do TR à evidência apresentada, incluindo links, documentos anexos ou explicações detalhadas.
 - Pode-se incluir comentários sobre limitações, alternativas ou adaptações propostas.

ANEXO III - DO EDITAL

MODELO DE DECLARAÇÃO DE INEXISTÊNCIA DE PRÁTICAS DE NEPOTISMO

“DECLARAÇÃO”

Ref.: Licitação nº 022/2025- Pregão Eletrônico - Processo SEI nº 002350/2025

A empresa, inscrita no CNPJ nº, por intermédio de seu representante legal o Sr....., portador da carteira de identidade nº..... e do CPF nº, **DECLARA**, especialmente para a **Licitação nº 022/2025- Pregão Eletrônico - Processo SEI nº 002350/2025**, que em seu quadro societário não compõe nenhum integrante que sejam Sócios cônjuge, companheiro ou parente em linha reta ou colateral até o terceiro grau, inclusive, dos respectivos membros ou Conselheiros vinculados, ou servidor investido em cargo de direção e de assessoramento, conforme dispõe o art. 2º, inciso V, da Resolução CNJ n. 7.

Boa Vista-RR, _____ de _____ de 2026.

(representante legal)

ANEXO IV - DO EDITAL

MINUTA DE CONTRATO

Processo nº 002350/2025

CONTRATANTE
- TRIBUNAL
DE CONTAS
DO ESTADO
DE
RORAIMA,
pessoa jurídica
de direito
público, com
sede na Rua.
Prof. Agnelo
Bitencourt, nº
126, centro,
nesta capital,
inscrito no
CNPJ nº
84.008.440/0001-
85, neste ato
representado
pelo Senhor
Amélio Valmir
Martini
Machado,
Diretor de
Gestão
Administrativa e
Financeira,
autorizado por
meio da Portaria
nº
60/2025/TCE-
RR.

CONTRATADA
– **(inserir**
nome), pessoa
jurídica de
direito privado,
inscrita no
CNPJ nº (inserir
dados),
estabelecida
comercialmente
na (inserir
endereço do
estabelecimento),
neste ato
representada
pelo (inserir
denominação),
Senhor(a)
(inserir nome),
portador do CPF
nº (inserir
dados) e RG nº
(inserir dados).

1. CLÁUSULA PRIMEIRA - DO OBJETO

Contratação de serviços de gerenciamento de Firewall de Borda, WAF (Web Application Firewall) e SOC (Security Operations Center), incluindo suporte técnico remoto e especializado, para atendimento à infraestrutura de tecnologia da informação do Tribunal de Contas do Estado de Roraima (TCERR).

2. CLÁUSULA SEGUNDA - DA DESCRIÇÃO DO OBJETO E VALORES

2.1. O valor da contratação é de R\$....

2.2. Segue abaixo as especificações do objeto do contrato:

GRUPO 1 [FIREWALL]					
Item	Descrição dos Serviços	Unidade.	Quantidade	Valor Unitário R\$	Valor Total R\$
1	Serviço de Gerenciamento de Tecnologia de Segurança de Rede (UTM-NGFW) , garantia e suporte técnico pelo período de 60 meses , com disponibilidade de 2 equipamentos em regime de comodato	Serv./mês	60		
2	Serviço de Gerenciamento de Tecnologia de Segurança de Rede Aplicação WEB (WAF - Web Application Firewall) , garantia e suporte técnico pelo período de 60 meses , com disponibilidade de equipamentos em regime de comodato.	Serv./mês	60		
3	Solução de Relatoria , garantia e suporte técnico pelo período de 60 meses .	Serv./mês	60		
4	Serviço de Implantação, Migração e Configuração.	Serv	1		
5	Serviço de Treinamento de equipe técnica do Contratante.	Serv	1		
6	Serviços Técnicos Especializados em Segurança da Informação (sob demanda)	UST	120		
Preços Globais do GRUPO 01 R\$					

Tabela 1 - Valor de Firewall Grupo 1

GRUPO 2 [SOC]					
Item	Descrição dos Serviços	Unidade.	Quantidade	Valor Unitário R\$	Valor Total R\$
7	Serviço de SOC 24x7 com SIEM, período de 36 meses	Serv./mês	36		
8	Serviços Técnicos Especializados (SOC) (sob demanda) pelo período de 36 meses .	UST	1080		
Preços Globais do GRUPO 02 R\$					

Tabela 2 - Valor de SOC Grupo 2

2.3. As especificações técnicas constam nos anexos do Termo de Referência.

3. CLÁUSULA TERCEIRA - DO REGIME DE EXECUÇÃO

O objeto do presente termo será executado de forma indireta, sob o regime de **empreitada por preço global**.

4. CLÁUSULA QUARTA - DA FORMA DE EXECUÇÃO DO SERVIÇO

O fornecimento será realizado em duas etapas, organizadas em grupos distintos, conforme descrito a seguir.

4.1. Grupo 1 - FIREWALL (Itens 1 a 6):

4.1.1. Os prazos para execução do **Grupo 1** estão estabelecidos na tabela abaixo:

ETAPA	EVENTOS	PRAZO
ETAPA 1	- Entrega do Equipamento - Instalação física da solução	45 dias após a assinatura do contrato
ETAPA 2	- Reunião "Kick-off" - Levantamento de requisitos e configurações atuais - Levantamento do ambiente e projeto de migração dos dados	5 dias após ETAPA 1
ETAPA 3	- Implantação das configurações da Solução e Migração	15 dias após a ETAPA 2
ETAPA 4	- Treinamento	10 dias após a ETAPA 3

Tabela 3 - Requisitos Temporais Grupo 1

4.1.2. O software e as subscrições contratadas deverão ser fornecidos antes do final da Etapa 2.

4.2. Grupo 2 - SOC (Itens 7 e 8):

4.2.1. Os prazos para execução do **Grupo 2** estão estabelecidos na tabela abaixo:

ETAPA	EVENTOS	PRAZO
ETAPA 1	- Reunião "Kick-off" - Levantamento de requisitos e ativos. - Levantamento do ambiente e projeto para implantação do SIEM.	15 dias após a assinatura do contrato
ETAPA 2	- Implantação do SIEM - Configuração dos ativos.	30 dias após a ETAPA 1
ETAPA 3	- Disponibilização do Software para acompanhamento do Monitoramento	15 dias após a ETAPA 2

Tabela 4 - Requisitos Temporais Grupo 2

4.2.2. Os prazos de execução detalhados nas Tabelas 3 e 4 são contados a partir da assinatura do contrato, respeitando a sequência das etapas e garantindo o pleno atendimento dos requisitos previstos no Termo de Referência.

4.3. NÍVEIS DE SERVIÇO - Grupo 1 - Firewall (Itens 1 a 6) - (SLA):

4.3.1. Para manutenção do desempenho da Contratada será adotado o **SLA (Service Level Agreement/Acordo de Nível de Serviço)** cujos critérios estão a seguir estabelecidos.

4.3.2. Deve ser considerado o regime de atendimento 8 X 5 em horário comercial das 8:00 às 18:00 horas (horário de Brasília), de segunda à sexta-feira, exceto feriados.

4.3.3. O nível de desempenho no atendimento terá como referência os prazos máximos para resposta aos acionamentos, contados a partir do momento da abertura do chamado, de acordo com os Níveis de Severidade dos Chamados e Tabela de Prazos de Atendimento, conforme quadros abaixo:

NÍVEIS DE SEVERIDADE DOS CHAMADOS

GRAU	DESCRIÇÃO DO EVENTO	TEMPO PARA PRIMEIRO CONTATO APÓS ABERTURA DE CHAMADO	TEMPO DE RESOLUÇÃO DO CHAMADO	VALOR A SER GLOSADO
------	---------------------	--	-------------------------------	---------------------

BAIXO	Serviços disponíveis com ocorrência de falhas ocasionais, consulta sobre problemas, dúvidas gerais. Pequeno impacto. Falha de componentes que não impactam o ambiente da Contratante.	90 minutos	Até 06 (seis) horas	0,2% do valor mensal do contrato por hora de atraso injustificado, até o limite de 10%.
URGENTE	Equipamento parcialmente indisponível ou com diminuição da performance de funcionamento. Falha intermitente que torne o ambiente inoperante. Operação afetada, mas sem interrupção das operações críticas da Contratante.	60 minutos	Até 04 (quatro) horas	0,5% do valor do contrato por hora de atraso injustificado, até o limite de 10%.
CRÍTICO	Equipamento totalmente inoperante, afetando operações críticas da Contratante. Problemas em funcionalidades essenciais.	30 minutos	Até 02 (duas) horas	1% do valor mensal do contrato por hora de atraso injustificado, até o limite de 10 %.

Tabela 5 - Níveis de Severidade dos Chamados - Grupo 1

4.3.4. A Contratada deverá informar o número do chamado e disponibilizar um meio de acompanhamento e evolução até a conclusão.

4.3.5. Entende-se por início do atendimento o primeiro contato, após abertura do chamado, feito pela Contratante para tratar do problema reportado.

4.3.6. Entende-se por término do atendimento a execução do serviço de correção e disponibilização do equipamento em perfeitas condições de funcionamento no local onde está instalado, tendo sanado todos os problemas relatados pela Contratante na abertura do chamado.

4.3.7. O nível de severidade será informado pela Contratante no momento da abertura de cada chamado.

4.3.8. O nível de severidade poderá ser reclassificado a critério da Contratante.

4.3.9. Nos casos de chamados classificados como Nível de Severidade “CRÍTICO”, o atendimento deverá ser contínuo até a resolução. Os prazos para as demais severidades podem ter sua contagem de tempo interrompida ao final de cada dia útil e reiniciada no primeiro dia útil subsequente.

4.3.10. Caso a solução definitiva requeira um tempo maior que o especificado na “**Tabela 5 - Níveis de Severidade dos Chamados - Grupo 1**”, seja devido à sua complexidade, ou por necessidade de ajustes nas configurações, modificações de software ou substituição do equipamento, uma solução de contorno deve ser sugerida e a severidade adequada à realidade da solução definitiva.

4.3.11. Ao final de cada atendimento, a Contratada deverá emitir relatório técnico contendo as seguintes informações: categoria de prioridade, descrição do problema e da solução, procedimentos realizados, data e hora da abertura e do fechamento do chamado, data e hora do início e término da execução dos serviços, identificação do técnico que realizou o atendimento.

4.3.12. As glosas apuradas em razão da aplicação do **SLA** ocorrerão no faturamento do mês subsequente.

4.3.13. As eventuais glosas no caso de descumprimento do **SLA** não devem ser interpretadas como penalidades, e sim como adequações pelo não atendimento das metas estabelecidas em complemento à mensuração dos serviços efetivamente prestados.

4.3.14. Após a 24^a (vigésima quarta) hora de atraso injustificado para o atendimento e solução do chamado técnico, o Contratante poderá rescindir o contrato, caracterizando-se a inexecução do objeto.

4.4. NÍVEIS DE SERVIÇO - Grupo 2 (Itens 7 e 8) - (SLA)

4.4.1. Para manutenção do desempenho da Contratada será adotado o **SLA (Service Level Agreement/Acordo de Nível de Serviço)** cujos critérios estão a seguir estabelecidos.

4.4.2. Deve ser considerado o regime de atendimento 24 x 7.

4.4.3. O nível de desempenho no atendimento terá como referência os prazos máximos para resposta aos acionamentos, contados a partir do momento da abertura do chamado, de acordo com a **Tabela 6 - Níveis de Severidade dos Chamados - Grupo 2**, conforme quadro abaixo:

NÍVEIS DE SEVERIDADE DOS CHAMADOS

GRAU	DESCRIÇÃO DO EVENTO	SLA PARA DETECÇÃO	SLA PARA RESPOSTA	SLA PARA SOLUÇÃO	VALOR A SER GLOSADO
BAIXO	Alertas falsos, solicitações de suporte técnico, ou eventos de baixa criticidade	Até 4 (quatro) horas	Até 8 (oito) horas	Até 48(quarenta e oito) horas	0,5% do valor mensal do contrato por hora de atraso injustificado, até o limite de 10%.
URGENTE	Ameaça significativa à operação: de sistemas não críticos, perda de dados não confidenciais, ou degradação do desempenho	Até 2 (duas) horas	Até 04 (quatro) horas	Até 6 (seis) horas	1% do valor mensal do contrato por hora de atraso injustificado, até o limite de 10%.
CRÍTICO	Ameaça imediata a sistemas críticos: perda de dados confidenciais, ou interrupção e serviços essenciais	Até 1 (uma) hora	Até 02 (duas) horas	Até 4 (quatro) horas	2% do valor mensal do contrato por hora de atraso injustificado, até o limite de 10%

Tabela 6 - Níveis de Severidade dos Chamados - Grupo 2

4.4.4. O SLA da disponibilidade do serviço terá como referência as metas definidas na tabela abaixo:

Indicador	Meta	Base para Penalidade	Penalidade
Disponibilidade do suporte técnico	24x7	Indisponibilidade do suporte	1% do valor mensal do contrato por hora de indisponibilidade
Relatório de incidente de segurança	Até 05 dias úteis após a conclusão do incidente	Atraso na entrega	0,5% do valor mensal do contrato por dia de atraso
Disponibilidade do serviço	24x7	Tempo de indisponibilidade	1% do valor mensal do contrato por hora de indisponibilidade
Conclusão do monitoramento de ativos	Até 90 (noventa) dias do início da execução do contrato	Atraso na implantação do monitoramento	0,5% do valor mensal do contrato por dia de atraso

Tabela 7 - Disponibilidade do Serviço

4.4.5. A Contratada deverá informar o número do chamado e disponibilizar um meio de acompanhamento e evolução até a conclusão.

4.4.6. Entende-se por início do atendimento o primeiro contato, após abertura do chamado, feito pela Contratante para tratar do problema reportado.

4.4.7. Entende-se por término do atendimento a execução do serviço de correção, tendo sanado todos os problemas relatados pela Contratante na abertura do chamado.

4.4.8. O nível de severidade será informado pela Contratante no momento da abertura de cada chamado.

4.4.9. O nível de severidade poderá ser reclassificado a critério da Contratante.

4.4.10. Nos casos de chamados classificados como Nível de Severidade “CRÍTICO”, o atendimento deverá ser contínuo até a resolução. Os prazos para as demais severidades podem ter sua contagem de tempo interrompida ao final de cada dia útil e reiniciada no primeiro dia útil subsequente.

4.4.11. Caso a solução definitiva requeira um tempo maior que o especificado na “**Tabela 6- Níveis de Severidade dos Chamados - Grupo 2**”, seja devido à sua complexidade, ou por necessidade de ajustes nas configurações, modificações de software ou substituição do equipamento, uma solução de contorno deve ser sugerida e a severidade adequada à realidade da solução definitiva.

4.4.12. Ao final de cada atendimento, a Contratada deverá emitir relatório técnico contendo as seguintes

informações: categoria de prioridade, descrição do problema e da solução, procedimentos realizados, data e hora da abertura e do fechamento do chamado, data e hora do início e término da execução dos serviços, identificação do técnico que realizou o atendimento.

4.4.13. As glosas apuradas em razão da aplicação do **SLA** ocorrerão no faturamento do mês subsequente.

4.4.14. As eventuais glosas no caso de descumprimento do **SLA** não devem ser interpretadas como penalidades, e sim como adequações pelo não atendimento das metas estabelecidas em complemento à mensuração dos serviços efetivamente prestados.

4.4.15. Após a 24ª (vigésima quarta) hora de atraso injustificado para o atendimento e solução do chamado técnico, o Contratante poderá rescindir o contrato, caracterizando-se a inexecução do objeto.

4.4.16. O monitoramento e a apuração dos **SLAs** serão realizados com base nos dados extraídos das ferramentas e plataformas utilizadas pela CONTRATADA, as quais deverão estar disponíveis ao TRIBUNAL DE CONTAS DE RORAIMA para fins de validação, fiscalização e auditoria.

4.5. Requisitos de Suporte Técnico, Manutenção e Garantia.

4.5.1. Suporte Técnico:

4.5.1.1. O serviço de suporte técnico à solução destina-se:

- a) A Instalação, configuração, correção de problemas e esclarecimento de dúvidas sobre configuração e utilização da solução ofertada;
- b) A empresa deve possuir no momento da assinatura do contrato, pelo menos 1 (um) profissional com certificação técnica emitida pelo fabricante, capaz de prestar o Serviço Especializado;
- c) A CONTRATADA é responsável pelo gerenciamento dos chamados e fornecimento de informações à CONTRATANTE, mesmo que haja escalonamento ao fabricante.

4.5.2. Manutenção dos Equipamentos (Grupo 1):

4.5.2.1. A contratada deverá prestar o serviço de manutenção dos equipamentos do Grupo 1 (Itens 1 e 2) durante a vigência do contrato.

4.5.2.2. Os equipamentos deverão possuir garantia do fabricante de **60 (sessenta) meses** para entrega de peças *on-site* em Boa Vista/RR.

4.5.2.3. O(s) fabricante(s) deverá(ão) emitir os Termos de Garantia dos equipamentos a serem fornecidos pela Contratada.

4.5.2.4. A empresa a ser Contratada poderá substituir o equipamento danificado por outro novo com especificações similares ou superiores, a seu critério, desde que tal substituição seja aprovada pela equipe técnica do TCERR e não represente qualquer tipo de prejuízo ao erário.

4.5.2.5. Manutenção corretiva: Entende-se por manutenção corretiva a série de procedimentos destinados a recolocar os equipamentos em seu perfeito estado de uso, compreendendo, inclusive, substituições de peças, ajustes e reparos necessários, de acordo com os manuais e normas técnicas específicas para os equipamentos.

4.5.2.6. Na ocorrência de manutenção corretiva, os componentes substitutos deverão ser novos, sem utilização anterior, com configuração igual ou superior aos originais e em linha de produção. Caso o componente não se encontre mais disponível no mercado, deve-se observar que o componente substituto deve ter, no mínimo, a mesma qualidade e especificações técnicas do componente fora de linha.

4.5.2.7. Sendo constatada a necessidade de substituição do equipamento pela equipe de suporte técnico da Contratada, o procedimento será efetuado sem qualquer ônus para a Contratante.

4.5.2.8. Manutenção preventiva: Entende-se por manutenção preventiva aquela que é realizada periodicamente para evitar paradas e manter o equipamento em condições de trabalho normal, programada em comum acordo com a Contratante, de modo a evitar ao máximo a indisponibilidade dos equipamentos contratados.

4.5.2.9. Na realização da manutenção preventiva a Contratada deverá realizar revisões, testes e adequações nos equipamentos visando a garantir o melhor desempenho da solução contratada.

4.5.2.10. Serão executadas, no mínimo, **2 manutenções preventivas** a cada período de **12 meses** de contrato, sem ônus adicional à Contratante.

4.5.2.11. Caso, para a solução do problema, seja necessária a retirada do equipamento das dependências do prédio

sede desta Corte, a Contratada poderá fazê-lo exclusivamente às suas expensas, mantendo inalterado o prazo para conclusão do trabalho.

4.5.2.12. Na hipótese de produto que necessite de peças ou partes importadas e não comuns de mercado, a critério da fiscalização do contrato, o prazo para a conclusão dos trabalhos poderá ser ampliado.

4.5.3. Requisitos de Negócio:

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

4.5.3.1.1 Garantir que a infraestrutura da rede de dados do TCERR seja monitorada e melhorada, permitindo melhor defesa a ataques cibernéticos;

4.5.3.1.2. Garantir a disponibilidade, continuidade e qualidade dos serviços para o cumprimento das atividades finalísticas do Tribunal e, conseqüentemente, o alcance dos resultados desejados para a sociedade;

4.5.3.1.3. Garantir os meios adequados para que os processos de segurança da informação possam ser aprimorados através da implementação de recursos de proteção adequados.

4.5.4. Requisitos de Capacitação - Grupo 1

4.5.4.1. O treinamento à equipe local do Tribunal será realizado na modalidade presencial, preferencialmente nos períodos das 08:00 às 12:00 e das 14:00 às 18:00, em dias úteis e em horário a ser definido pelo Tribunal;

4.5.4.2. O treinamento deverá ter uma **carga horária mínima de 16 horas**;

4.5.4.3. A contratada deverá ministrar treinamento para até 5 participantes da equipe técnica da Contratante;

4.5.4.4. O treinamento deverá abranger o repasse de informações e conhecimentos referentes à administração e gerenciamento da solução Itens (1,2 e 3), bem como o esclarecimento de dúvidas.

4.5.4.5. O treinamento deverá ser ministrado em língua portuguesa por profissional certificado pelo fabricante do produto ofertado.

5. PRAZO E LOCAL DE ENTREGA

5.1. O prazo para início da execução contratual será a partir da assinatura do contrato, devendo, a partir desse momento, seguir o cronograma detalhado de execução das etapas, conforme **cláusula quarta**.

5.2. Os prazos específicos de entrega, instalação, implantação e treinamento seguirão as etapas e prazos estabelecidos nas Tabelas 3 e 4 da cláusula quarta.

5.3. O local de entrega, instalação e execução dos serviços relacionados ao **Grupo 1** será nas dependências do Tribunal de Contas do Estado de Roraima (TCERR), ou em outro local que venha a ser formalmente indicado pela Contratante.

5.4. O prazo de entrega do objeto poderá ser prorrogado de forma excepcional, mediante justificativa fundamentada e aprovação da fiscalização do contrato, observando os limites previstos na Lei nº 14.133/2021.

6. CLÁUSULA SEXTA - DA GARANTIA E ASSISTÊNCIA TÉCNICA

Os requisitos de garantia e assistência técnica estão detalhados no *item 4.5. Requisitos de Suporte Técnico, Manutenção e Garantia*.

7. CLÁUSULA SÉTIMA - DA VIGÊNCIA DO CONTRATO

7.1. O prazo de vigência do contrato será contado a partir da assinatura, podendo ser prorrogado nos termos do art. 107 da Lei nº 14.133/2021, com as seguintes especificações:

7.1.1. **Grupo 1 – Firewall:** vigência de **60 meses** para fornecimento, manutenção e suporte dos equipamentos e softwares relacionados.

7.1.2. **Grupo 2 – SOC:** vigência de **36 meses** para prestação de serviços de monitoramento, suporte e atendimento remoto.

7.2. A gestão contratual, eventuais prorrogações, fiscalizações e encerramentos de cada grupo serão conduzidos de forma **autônoma**, observando-se seus respectivos prazos e condições específicas.

7.3. Havendo interesse, a vigência do contrato poderá ser prorrogada condicionada a:

7.3.1. Preços e condições vantajosas;

7.3.2. Regularidade fiscal e trabalhista;

7.3.3. Inexistência de sanção impeditiva, comprovada por meio da consulta no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e Cadastro Nacional de Empresas Punidas (CNEP), podendo ser substituídas pela Consulta Consolidada no portal do Tribunal de Contas da União (TCU).

7.4. A vigência contratual de cada grupo de serviços terá início a partir da data da última assinatura das partes no termo de contrato, sendo a contagem do prazo **independente para cada grupo**, conforme seus respectivos cronogramas e especificações.

8. CLÁUSULA OITAVA - DO MODELO DE GESTÃO DO CONTRATO

8.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas contidas na Lei nº 14.133/2021, onde cada parte responderá pelas consequências do seu descumprimento, seja parcial ou total.

8.2. A execução do contrato será acompanhada e fiscalizada por fiscal ou equipe de fiscalização devidamente designada para esse fim, com atribuições de representar administrativamente o Contratante e proceder o recebimento do objeto quando não designada comissão de recebimento.

8.3. As competências e atribuições do fiscal e da equipe de fiscalização estão regulamentadas por meio da **Resolução nº 20/2023/TCERR-PLENO**, ep. 0843916.

8.4. O Contratado deverá informar imediatamente à fiscalização fato que impeça o cumprimento tempestivo da entrega ou execução do objeto.

8.5. Nos contratos por escopo, o Contratado deverá manter o Contratante sempre informado acerca do andamento da entrega do objeto, devendo disponibilizar, sempre que possível, os dados de rastreio para acompanhamento.

8.6. As comunicações entre o Contratante e o Contratado que exigirem formalidade de atos deverão ser realizadas sempre por meio eletrônico.

8.7. Identificada qualquer inexatidão ou irregularidade no cumprimento das cláusulas contratuais, o responsável pela fiscalização emitirá notificações para a correção, determinando prazo adequado para tal ato.

8.8. Caso ocorram descumprimento das obrigações contratuais, o responsável pela fiscalização atuará tempestivamente na solução do problema, reportando os fatos ao gestor de contratos para que tome as providências cabíveis, quando ultrapassar a sua competência.

8.9. Havendo injustificado inadimplemento contratual, o responsável pela fiscalização autuará processo administrativo específico para a apuração da conduta faltosa do Contratado, observando as diretrizes contidas na **Resolução nº 002/2024-TCERR-PLENO**, ep. 1034993.

9. CLÁUSULA NONA - DA FORMA E CONDIÇÕES DE RECEBIMENTO

9.1. O objeto contratual será recebido pelo fiscal do contrato ou pela equipe designada, conforme as etapas previstas para o **Grupo 1 (Firewall)** e o **Grupo 2 (SOC)**, observando os prazos estabelecidos nas respectivas tabelas de requisitos temporais (itens 7.1.1. e 7.1.2.)

9.1.1 Recebimento Provisório

9.1.1.1 Grupo 1 – Firewall: ocorrerá após a conclusão da ETAPA 2 conforme cronograma da Tabela 3, ou seja, 50 (cinquenta) dias após a assinatura do contrato.

9.1.1.2 Grupo 2 – SOC: ocorrerá após a conclusão da ETAPA 2 conforme cronograma da Tabela 4, ou seja, 45 (quarenta e cinco) dias após a assinatura do contrato.

9.1.2 Recebimento Definitivo

9.1.2.1 Grupo 1 – Firewall: até 10 (dias) úteis após a conclusão da ETAPA 3 conforme cronograma da Tabela 3.

9.1.2.2 Grupo 2 – SOC: até 10 (dias) úteis após a conclusão da ETAPA 3 conforme cronograma da Tabela 4.

9.2. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, desde que justificado junto ao fiscal do contrato.

9.3. Os bens entregues poderão ser rejeitados no todo ou em parte, inclusive antes do recebimento provisório, quando estiverem em desacordo com as especificações constantes no Termo de Referência e proposta adjudicada,

devendo ser substituídos às custas do Contratado no prazo de até **10 dias úteis**, a contar da notificação, sem prejuízo da aplicação das penalidades cabíveis.

9.4. O prazo para o saneamento de inconsistências na execução do objeto não será computado para os fins de recebimento definitivo.

9.5. O recebimento provisório ou definitivo não exclui a responsabilidade pelas obrigações contratuais posteriores e garantia pertinente ao objeto.

9.6. Por se tratar de serviço continuado, executado por demand e com pagamento mensal, a liquidação deverá, ao final de cada mês, ser instruída minimamente com: 1) Nota Fiscal; 2) Atesto; 3) Relatório de Acompanhamento; e 4) Despacho de Liquidação e Pagamento, dirigido à Unidade competente.

10. CLÁUSULA DÉCIMA - DA FORMA E CONDIÇÕES DE PAGAMENTO

10.1. Condições de Pagamento por Grupo e Natureza do Serviço:

10.1.1. **Grupo 1 (FIREWALL) - Serviços Contínuos (Itens 1, 2 e 3):** O pagamento será efetuado mensalmente, durante 60 meses, ao final de cada período de execução dos serviços contínuos, mediante a conclusão e aceite dos serviços prestados, conforme critérios estabelecidos no Item 10 (Forma e Condições de Recebimento).

10.1.2. **Grupo 1 (FIREWALL) - Serviços de Implantação e Treinamento (Itens 4 e 5) :** O pagamento referente aos serviços de Implantação, Migração e Configuração (Item 4) e Treinamento da equipe técnica (Item 5) será realizado após a conclusão e aceite da ETAPA 4 (Treinamento), conforme cronograma estabelecido na Tabela 3.

10.1.3. **Grupo 1 (FIREWALL) - Serviços Sob Demanda (Item 6):** O pagamento pelos Serviços Técnicos Especializados em Segurança da Informação (Item 6) será efetuado por demand, mediante a emissão prévia de Ordens de Serviço (OS) e após a entrega dos serviços com respectivo relatório de execução, referente a 120 UST distribuídas ao longo do período de 60 meses.

10.1.4. **Grupo 2 (SOC) - Serviços Contínuos (Item 7):** O pagamento será efetuado mensalmente, durante 36 meses, ao final de cada período de execução dos serviços contínuos, mediante a conclusão e aceite dos serviços prestados, conforme critérios do Item 14.

10.1.5. **Grupo 2 (SOC) - Serviços Sob Demanda (Item 8):** O pagamento pelos Serviços Técnicos Especializados (SOC) sob demand será realizado mediante a emissão prévia de Ordens de Serviço (OS) e entrega dos serviços com respectivo relatório de execução, referente a 1.080 UST distribuídas ao longo de 36 meses.

10.2. Para fins de pagamento, a nota fiscal eletrônica será encaminhada pelo Contratado, via *e-mail*, exclusivamente ao fiscal do contrato, cujo endereço eletrônico será repassado oportunamente.

10.3. Orientações para a emissão da nota fiscal ou documento equivalente para fins de retenção tributária:

10.3.1. O Contratado deverá observar quando da emissão da nota fiscal ou documento de cobrança equivalente às disposições da **Instrução Normativa RFB nº 1234/2012** alterada pela **Instrução Normativa RFB nº 2145/2023**, em especial o **art. 2º-A, parágrafos 2º e 3º** e os **arts. 3º e 11**, e os **anexos da instrução normativa** inicialmente citada, sem prejuízos do cumprimento das legislações pertinente ao INSS (União), ICMS (Estado) e ISS (Município);

10.3.2. As alíquotas dos tributos decorrentes da atividade empresarial do Contratado deverão constar expressamente no corpo da nota fiscal ou documento equivalente, bem como as informações acerca de eventual isenção tributária;

10.3.3. Em razão da extinção do convênio entre o Governo do Estado de Roraima e a União (DOU 219 de 22/11/2022 - Seção 3/Pag. 50), passam a ser de exclusiva responsabilidade do Contratado o recolhimento da **CSLL, COFINS e PIS/PASEP**.

10.4. Caso o Contratado não cumpra integralmente o disposto no item anterior, o pagamento não será processado até que ocorra a devida correção.

10.5. O Contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123/2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime, desde que apresente comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida lei complementar.

10.6. O pagamento ocorrerá em **até 10 dias úteis**, após o atesto da nota fiscal, por meio de ordem bancária para crédito no banco, agência e conta corrente indicados pelo Contratado.

10.7. Para fins de pagamento, o Contratado deverá estar adimplente com a Fazenda Federal e Estadual e/ou Municipal, incluindo a regularidade perante a Justiça do Trabalho e ao Fundo de Garantia por Tempo de Serviço

(FGTS).

10.8. Não será aceito como comprovação da regularidade fiscal perante a Fazenda Municipal a certidão emitida/validada na condição de contribuinte.

10.9. A nota fiscal que for apresentada com erro deverá ser imediatamente substituída, ficando o pagamento suspenso e o prazo para pagamento suspenso até que o Contratado providencie a substituição.

10.10. No preço contratado deverão estar inclusos todos os tributos, taxas, encargos, seguros, fretes e quaisquer outras despesas que incidam sobre o objeto.

10.11. No caso de atraso do pagamento, salvo se por culpa do Contratado, serão devidos pelo Contratante encargos moratórios à taxa nominal de 6% a.a. (seis por cento ao ano), capitalizados diariamente em regime de juros simples, conforme a seguinte fórmula: $EM = I \times N \times VP$, onde: EM = Encargos moratórios devidos. N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento. I = Índice de compensação financeira = 0,00016438. e VP = Valor do pagamento em atraso.

11. CLÁUSULA DÉCIMA PRIMEIRA - DA FORMA E CONDIÇÕES DE REAJUSTAMENTO

11.1. Os preços contratados poderão ser reajustados após 12 (doze) meses, contados da data do orçamento estimado de **23/10/2025**, com base na variação do **Índice de Custo da Tecnologia da Informação – ICTI**, divulgado pelo IPEA, ou de outro índice que venha a substituí-lo oficialmente, em conformidade com o [art. 92, §3º, da Lei nº 14.133/2021](#).

11.2. Para o cálculo do índice de reajustamento será adotada a seguinte **fórmula**:

$$IR = (if - ii) / ii$$

Onde:

IR = Índice de Reajustamento.

ii - índice inicial: índice do mês de apresentação da proposta.

if - índice final: índice correspondente a data do reajuste.

11.3. O reajuste de preços deverá ser solicitado formalmente pelo Contratado antes de eventual prorrogação do contrato, decaindo tal direito caso seja firmado termo aditivo prorrogatório sem a devida manifestação quanto ao reajuste.

11.4. Revisão de Preços:

11.4.1. A revisão dos preços contratados poderá ocorrer a qualquer tempo, com a finalidade de garantir a manutenção do equilíbrio econômico do contrato, podendo ocorrer da seguinte forma:

a) Pelo Contratante, nos casos em que for verificada a redução do preço praticado no mercado ou em decorrência de redução de carga tributária ou de estudos técnicos elaborados internamente;

b) Pelo Contratado, mediante solicitação formal e fundamentada e acompanhada da planilha de composição de custo do novo preço, contendo os mesmos elementos formadores dos preços contratados, devendo demonstrar quais os itens da planilha de custos estão defasados e que estão ocasionando o desequilíbrio do contrato.

11.4.2. Em nenhuma hipótese os preços revisados ultrapassarão os praticados no mercado.

11.4.3. Caso a revisão seja concedida, ocorrerá a partir da data da assinatura do respectivo termo aditivo, com efeitos financeiros a partir da data da solicitação do Contratado.

12. CLÁUSULA DÉCIMA SEGUNDA - DAS OBRIGAÇÕES DO CONTRATADO

12.1. Providenciar, imediatamente após o recebimento da nota de empenho, as tratativas necessárias ao cumprimento célere do encargo disposto neste Termo.

12.2. Prestar os serviços no prazo pactuado, sob pena de aplicação das penalidades previstas neste Termo.

12.3. Prestar a garantia necessária dos serviços conforme solicitado neste Termo de Referência.

12.4. Disponibilizar pessoal qualificado e habilitado para a execução dos serviços, conforme indicado no item 7.5.1.1.b e 24.4 do presente instrumento;

12.5. A CONTRATADA obriga-se a manter a estabilidade da equipe técnica envolvida nos projetos, providenciando a substituição de colaboradores que eventualmente se desliguem da equipe, garantindo o padrão

técnico e a qualidade dos trabalhos.

12.6. Decidir em comum acordo com a CONTRATANTE sobre os métodos, detalhes e meios através dos quais os serviços serão executados, utilizando pessoal com qualificação técnica necessária e em número suficiente para atender a demanda;

12.7. Fornecer à CONTRATANTE, sempre que formalmente solicitado, informações detalhadas sobre o andamento dos serviços;

12.8. Reparar, corrigir ou substituir, às suas expensas, no total ou em parte, os serviços em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados;

12.9. Responder, integralmente, por perdas e danos que vier a causar ao contratante ou à terceiros em razão de ação ou omissão, dolosa ou culposa, de seus empregados, independente de outras cominações contratuais ou legais a que estiver sujeita;

12.10. Entregar, ao final de períodos estabelecidos em comum acordo pelas partes, toda a documentação oriunda da execução das atividades relacionadas ao presente contrato.

12.11. A CONTRATADA obriga-se a manter a confidencialidade das informações compartilhadas e que não sejam de domínio público, além daqueles referentes ao conteúdo e tecnologia envolvida no projeto, exceto quando autorizado por escrito pela CONTRATANTE.

12.12. Manter durante toda a execução do contrato as condições de habilitação e qualificação exigidas no procedimento licitatório, devendo comunicar ao Contratante a superveniência de fato impeditivo da manutenção dessas condições.

12.13. Não subcontratar o objeto do presente Termo.

13. CLÁUSULA DÉCIMA TERCEIRA - DAS OBRIGAÇÕES DO CONTRATANTE

13.1. Efetuar o pagamento no prazo informado neste termo.

13.2. Acompanhar e fiscalizar a execução do contrato por meio de servidor designado para esse fim.

13.3. Verificar o cumprimento das especificações exigidas, podendo rejeitá-las quando não atenderem este termo.

13.4. Prestar informações necessárias ao Contratado para a perfeita execução do contrato.

14. CLÁUSULA DÉCIMA QUARTA - DA GARANTIA CONTRATUAL

14.1. Com a finalidade de assegurar a execução do contrato e suprir eventual situação de inadimplência, o Contratado apresentará **garantia contratual** na forma do art. 96 da Lei nº 14.133/2021, em até **30 dias**, após a homologação do certame e antes da assinatura do contrato, no percentual de **5%** do valor da contratação, podendo optar por uma das **modalidades de garantia** abaixo:

14.1.1. **Caução em Dinheiro:** a garantia em dinheiro deverá ser efetuada, obrigatoriamente, em conta específica, em favor do Contratante;

14.1.2. **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;

14.1.3. **Seguro Garantia:** será realizado mediante a entrega da apólice, inclusive digital, emitida por empresa em funcionamento no Brasil e devidamente registrada na Superintendência de Seguros Privados - SUSEP, sendo a Contratante o único beneficiário/segurado, observando-se, ainda, as disposições do art. 97 da Lei nº 14.133/2021;

14.1.4. **Fiança Bancária:** mediante entrega de carta de fiança fornecida por estabelecimento bancário, devidamente registrada em cartório de registro de títulos e documentos, conforme determinado no art. 129 da Lei nº 6.015/73. Na Fiança Bancária, deverá constar do instrumento a expressa renúncia pelo fiador dos benefícios previstos nos artigos 827 e 835 do Código Civil Brasileiro;

14.1.5. **Título de capitalização** custeado por pagamento único, com resgate pelo valor total.

14.2. **A garantia contratual assegurará, qualquer que seja a modalidade escolhida, o pagamento de:**

14.2.1. Prejuízos advindos do não cumprimento do contrato e do não adimplemento das demais obrigações nele previstas;

14.2.2. Prejuízos causados à Administração ou a terceiro, decorrentes de culpa ou dolo durante a execução do contrato;

14.2.3. Multas moratórias e punitivas aplicadas pelo Contratante; e

14.2.4. Obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza não adimplidas pelo Contratado, conforme a natureza do contrato.

14.3. Os dados do contrato garantido e/ou assegurado deverão constar no instrumento de garantia ou seguro a ser apresentado pelo garantidor e/ou segurador.

14.4. A garantia contratual terá validade mínima de **90 dias** além da vigência contratual, devendo ser renovada e atualizada no caso de alteração do valor e/ou prorrogação do contrato.

14.5. A garantia contratual será liberada ou restituída somente após a comprovação de que o Contratado cumpriu as obrigações contratuais.

15. CLÁUSULA DÉCIMA QUINTA - DAS SANÇÕES ADMINISTRATIVAS

15.1 Comete infração administrativa no âmbito da execução do contrato, nos termos da Lei nº 14.133/2021, o Contratado que:

15.1.1. dar causa à inexecução parcial do contrato;

15.1.2. dar causa à inexecução parcial do contrato, que cause grave dano ao Contratante;

15.1.3. dar causa à inexecução total do contrato;

15.1.4. ensejar o retardamento da execução ou da entrega do objeto sem motivo justificado;

15.1.5. prestar declaração falsa durante a execução do contrato;

15.1.6. praticar ato fraudulento na execução do contrato;

15.1.7. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

15.1.8. praticar ato lesivo previsto no art. 5º da Lei nº 12.846/2013.

15.2. O Contratado que cometer quaisquer das infrações discriminadas no item 15.1 ficará sujeito, sem prejuízo das responsabilidades civil e criminal, às seguintes sanções:

15.2.1 **ADVERTÊNCIA:** no caso de cometimento da infração administrativa prevista no **subitem 15.1.1**, quando **não se justificar** a imposição de penalidade mais grave.

15.2.2. **MULTA:**

a) de **10%** sobre o valor do contrato no caso de cometimento das infrações administrativas previstas nos **subitens 15.1.1 e 15.1.4;**

b) de **15%** sobre o valor do contrato no caso de cometimento das infrações administrativas previstas nos **subitens 15.1.2 e 15.1.3;**

c) de **20%** sobre o valor do contrato no caso de cometimento das infrações administrativas previstas nos **subitens 15.1.5 a 15.1.8.**

15.2.3. **MULTA MORATÓRIA :** de **0,5%** sobre o valor do contrato ou item, **por dia de atraso injustificado** na execução do objeto, limitada a **30%** , podendo ser convertida em **multa compensatória** no caso de extinção unilateral do contrato, sem prejuízo da aplicação cumulativa com outras sanções previstas em lei.

15.2.3.1. Não havendo **garantia contratual**, ocorrerá a **retenção preventiva** do valor presumido da **multa moratória** antes da instauração do regular procedimento administrativo;

15.2.3.2. Se a **multa** aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada, se houver, ou será cobrada judicialmente.

15.2.4. **IMPEDIMENTO DE LICITAR E CONTRATAR:** pelo prazo de **2 anos**, no caso de cometimento das infrações administrativas previstas nos **subitens 15.1.2 e 15.1.3**, e de **6 meses**, no caso de cometimento da infração administrativa previstas no **subitem 15.1.4**, quando **não se justificar** a imposição de penalidade mais grave.

15.2.5. **DECLARAÇÃO DE INIDONEIDADE:** pelo prazo de **3 anos**, no caso de cometimento das infrações administrativas previstas nos **subitens 15.1.5 e 15.1.6**, e de **6 anos**, no caso de cometimento da infração administrativa previstas no **subitens 15.1.7 e 15.1.8**, bem como pelo prazo de **3 anos**, no caso de cometimento das infrações **15.1.2 a 15.1.4**, quando **se justificar** a imposição de penalidade mais grave.

15.2.6. As sanções previstas nos **subitens 15.2.1, 15.2.4 e 15.2.5** poderão ser aplicadas **cumulativamente** com a prevista no **subitem 15.2.2**.

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

15.4. O exercício do direito ao **contraditório** e a **ampla defesa** acerca da imputação das infrações previstas neste item ocorrerá no âmbito do **processo administrativo sancionatório**.

15.5. O **processo administrativo sancionatório** seguirá às disposições da **Resolução nº 02/2024-TCERR-PLENO**.

15.6. No caso de abertura de **processo administrativo sancionatório** destinado a apuração de infrações contratuais e eventual aplicação de sanção administrativa, as comunicações ao Contratado serão realizadas preferencialmente por meio do endereço de correio eletrônico (e-mail) informado na proposta adjudicada ou o constante no Sistema de Cadastro Unificado de Fornecedores (SICAF).

15.6.1. O Contratado deverá manter atualizado o endereço de correio eletrônico (e-mail) informado na proposta e no Sistema de Cadastro Unificado de Fornecedores (SICAF), e confirmar o recebimento das mensagens provenientes do Tribunal de Contas do Estado de Roraima, não podendo alegar o desconhecimento do recebimento das comunicações por este meio como justificativa para se eximir das responsabilidades assumidas ou de eventuais sanções aplicadas.

16. CLÁUSULA DÉCIMA SEXTA - DA PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

16.1. As partes se comprometem a proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, relativos ao tratamento de dados pessoais, nos termos da Lei Geral de Proteção de Dados - LGPD (Lei nº 13.709/2018).

16.2. O Contratado obriga-se ao dever de proteção, confidencialidade, sigilo da informação, dados pessoais e base de dados a que tiver acesso, nos termos da LGPD em razão da execução do contrato.

16.3. O Contratado não poderá utilizar informações, dados pessoais ou base de dados a que tenham acesso para fins distintos da execução do contrato.

16.4. Caso o Contratado necessite coletar dados pessoais dos titulares mediante consentimento, indispensáveis a execução do contrato, esta será realizada após prévia aprovação do Contratante, sendo de sua exclusiva responsabilidade a obtenção e gestão desses dados.

16.5. Os dados obtidos em razão deste contrato deverão ser armazenados em banco de dados seguro, com garantia de registro das transações realizadas na aplicação de acesso (log), adequado controle baseado em função (role based access control) e com transparente identificação do perfil dos credenciados, como forma de garantir a rastreabilidade de cada transação e a franca apuração, a qualquer momento, de desvios e falhas, vedado o compartilhamento desses dados com terceiros.

16.6. O Contratado se responsabiliza integralmente pela regularidade do tratamento dos dados pessoais recebidos do Contratante ou gerados durante a execução do contrato, desde o momento do seu acesso ou coleta, até o seu descarte, devendo cumprir as regras impostas pela Lei Geral de Proteção de Dados, nos regulamentos dela decorrentes e orientações de boas práticas publicadas pela Autoridade Nacional de Proteção de Dados.

16.7. O Contratado obriga-se a implementar medidas técnicas e administrativas aptas a promover a segurança, à proteção, a confidencialidade e o sigilo da informação, dados pessoais e/ou base de dados que tenha acesso, a fim de evitar acessos não autorizados, acidentes, vazamentos acidentais ou ilícitos que causem destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito.

16.8. O Contratado é responsável por assegurar que seus colaboradores, consultores, e/ou prestadores de serviços que, no exercício de suas atividades, tenham acesso e/ou conhecimento da informação e/ou dos dados pessoais, respeitem o dever de proteção, confidencialidade e sigilo, devendo estes assumir compromisso formal de preservar a confidencialidade e segurança de tais dados.

16.9. O Contratado deverá manter os registros de tratamento de dados pessoais que realizar em razão do contrato, assim como aqueles compartilhados, com condições de rastreabilidade e de prova eletrônica a qualquer tempo.

16.10. O Contratado deverá permitir a realização de auditorias pelo Contratante e disponibilizar as informações necessárias para demonstrar o cumprimento das obrigações relacionadas à Lei Geral de Proteção de Dados.

16.11. O Contratado deverá prestar, sempre que solicitado pelo Contratante, qualquer informação e documentação que comprovem a implementação dos requisitos de segurança especificados na contratação, de forma a assegurar a auditabilidade do objeto contratado, bem como os demais dispositivos legais aplicáveis.

16.12. Em casos de incidentes de segurança, o Contratado informará imediatamente via e-mail e telefone ao fiscal do contrato o ocorrido, devendo a comunicação conter, no mínimo, as seguintes informações:

16.12.1. Identificação e dados de contato de entidade ou pessoa responsável pelo tratamento; encarregado de dados ou outra pessoa de contato; indicação se a notificação é completa ou parcial. Em caso de comunicação parcial, indicar que se trata de uma comunicação preliminar ou de uma comunicação complementar;

16.12.2. Informações sobre o incidente de segurança com dados pessoais, tais como data e hora da ocorrência e duração do incidente, bem como de sua detecção;

16.12.3. A natureza da violação de segurança de dados pessoais, como por exemplo, perda, roubo, cópia, vazamento, dentre outros;

16.12.4. Descrição dos dados pessoais e informações afetadas, como natureza e conteúdo dos dados pessoais, categoria e quantidade de dados e de titulares afetados;

16.12.5. Indicação da localização física, meio de armazenamento e base de dados violada;

16.12.6. Possíveis consequências e efeitos negativos sobre os titulares dos dados afetados, indicando os titulares atingidos ou potencialmente atingidos;

16.12.7. Medidas de segurança, técnicas e administrativas preventivas tomadas pelo Controlador de acordo com a LGPD aplicadas ao incidente;

16.12.8. Resumo das medidas implementadas durante o processo de adequação e *compliance* com a LGPD para mitigação de riscos de incidentes desta natureza;

16.12.9. Outras informações úteis às pessoas afetadas para proteger seus dados ou prevenir possíveis danos.

16.13. Extinto o contrato, o Contratado interromperá o tratamento dos dados pessoais que porventura viesse ocorrendo em função do contrato, devendo eliminá-los no prazo máximo **30 dias**, salvo quando tenha que mantê-los para cumprimento de obrigação legal.

16.14. O Contratado é responsável pelos eventuais danos e sanções aplicadas pela Autoridade Nacional de Proteção de Dados, decorrentes do tratamento inadequado dos dados pessoais compartilhados pelo Contratante em razão do contrato.

16.15. O Contratado é responsável pelos danos patrimoniais, morais, individuais ou coletivos que venham a ser causados em razão do descumprimento de suas obrigações legais no processo de tratamento dos dados no âmbito do contrato.

17. CLÁUSULA DÉCIMA SÉTIMA - DA ADEQUAÇÃO ORÇAMENTÁRIA

A despesa decorrente da presente contratação correrá por conta da seguinte dotação:

- **Unidade Gestora:** Tribunal de Contas do Estado de Roraima
- **Projeto de Trabalho:** 01.032.002.2012.9900.
- **Fonte (s):** 1500.
- **Natureza da Despesa:** 3.3.90-40 - 3.3.90.40 – Serviços de Tecnologia da Informação e Comunicação.
- **Nota de Empenho:**

18. CLÁUSULA DÉCIMA OITAVA - DA FORMA DE ALTERAÇÃO CONTRATUAL

O contrato poderá ser alterado nos casos previstos no art. 124 da Lei 14.133/2021, desde que haja interesse do Contratante e as justificativas adequadas à situação.

19. CLÁUSULA DÉCIMA NONA - DA FORMA DE EXTINÇÃO DO CONTRATO

19.1. A rescisão do contrato ocorrerá motivadamente e com fundamento no art. 137 da Lei nº 14.133/2021, e se dará com observância nos artigos 138 e 139 da mesma norma.

19.1.1. No caso de rescisão provocada por inadimplemento da Contratada, o Contratante poderá reter, cautelarmente, os créditos decorrentes do contrato até o valor dos prejuízos causados, já calculados ou estimados.

19.2. No procedimento de rescisão contratual, será assegurado o contraditório e a ampla defesa à Contratada, que após formalmente intimada, terá o prazo decadencial de 15 dias úteis para manifestação.

20. CLÁUSULA VIGÉSIMA - DO AMPARO LEGAL

O presente contrato é regido pela Lei nº 14.133/2021 e tudo o que consta nos autos do Processo SEI 2350/2025.

21. CLÁUSULA VIGÉSIMA PRIMEIRA - DOS CASOS OMISSOS

Os casos omissos serão decididos pelo Contratante, segundo as disposições contidas na Lei nº 14.133/2021 e demais normas aplicáveis.

22. CLÁUSULA VIGÉSIMA SEGUNDA - DO FORO

Fica eleito o foro da cidade de Boa Vista como competente para dirimir dúvidas decorrentes deste contrato, com exclusão de qualquer outro, por mais privilegiado que seja.

AMÉLIO VALMIR MARTINI MACHADO Diretor de Gestão Administrativa e Financeira Representante do Contratante	(Inserir Nome) (inserir cargo) (Nome da Empresa) Representante da Contratada
--	---



Documento assinado eletronicamente por **AMELIO VALMIR MARTINI MACHADO, Diretor(a)**, em 12/12/2025, às 09:08, conforme horário oficial de Roraima, com fundamento na Resolução TCE/RR nº 06/2018, Portaria da Presidência-TCE/RR nº 744/2017.



A autenticidade deste documento pode ser conferida no site <https://sei.tcrr.tc.br/autenticar>, informando o código verificador **1159905** e o código CRC **63B6FBB7**.