PODER JUDICIÁRIO
TRIBUNAL REGIONAL FEDERAL DA 6ª REGIÃO
Seção de Licitações

EDITAL DE LICITAÇÃO

PREGÃO ELETRÔNICO 90017/2024
SISTEMA DE REGISTRO DE PREÇOS

CONTRATANTE (UASG): **TRF - 6ª Região - 090059**

OBJETO: **REGISTRO DE PREÇOS PARA AQUISIÇÃO DE SOLUÇÃO DE SEGURANÇA DE TIC COM A FINALIDADE DE ATENDER ÀS NECESSIDADES DE FUNCIONAMENTO DOS SISTEMAS DO TRIBUNAL REGIONAL FEDERAL DA 6ª REGIÃO.**

VALOR ESTIMADO DA CONTRATAÇÃO:
GRUPO 1: R$ 5.338.404,73
GRUPO 2: R$ 1.719.254,43
GRUPO 3: R$ 52.702.579,50

DATA DA SESSÃO PÚBLICA: **Dia 13/03/2025** às **13:30 h** **(horário de Brasília)**

Critério de Julgamento: **Menor preço**

Modo de disputa: **Aberto e fechado**

PREGÃO ELETRÔNICO Nº 90017/2024

SISTEMA DE REGISTRO DE PREÇOS

(PROCESSO ADMINISTRATIVO N° 0006130-19.2024.4.06.8000)

Torna-se público que o Tribunal Regional Federal da 6ª Região, por meio da Seção de Licitações - SELIT, sediado na Av. Álvares Cabral nº 1805 – Santo Agostinho – CEP: 30170-00, realizará licitação, **para registro de preços**, na modalidade PREGÃO, na forma ELETRÔNICA, nos termos da Lei 14.133/2021 , do Decreto nº 11.462, de 31 de março de 2023, da LC 123/06 e alterações, de acordo com as condições estabelecidas neste Edital e seus anexos.

1. DO OBJETO

1.1. O objeto da presente licitação é Registro de Preços para aquisição de solução de segurança de TIC com a finalidade de atender às necessidades de funcionamento dos sistemas do Tribunal Regional Federal da 6ª Região, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2. A licitação será dividida em 03 Grupos, formados por itens conforme tabela constante do item 18.3 do Termo de Referência, facultando-se ao licitante a participação em quantos grupos forem de seu interesse, devendo oferecer proposta para todos os itens que compõem cada grupo do qual esteja participando.

1.3. O critério de julgamento adotado será o menor preço, observadas as exigências contidas neste Edital e seus Anexos quanto às especificações do objeto.

1.4. Tratando-se de licitação em grupo, a contratação posterior de item específico do grupo exigirá prévia pesquisa de mercado e demonstração de sua vantagem para o órgão ou a entidade, e serão observados os preços unitários máximos indicados no item 18.3 do Termo de Referência, como critério de aceitabilidade.

2. DO REGISTRO DE PREÇOS

2.1. Ao **TRF - 6ª Região, na qualidade de entidade gerenciadora**, bem como aos órgãos ou entidades participantes e aos eventuais aderentes, **serão aplicadas as regras constantes da minuta da Ata de Registro de Preços - Anexo IV**, revestida de caráter vinculativo e obrigacional.

3. DA PARTICIPAÇÃO NA LICITAÇÃO

3.1. Poderão participar deste Pregão os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras), por meio de Certificado Digital conferido pela

Infraestrutura de Chaves Públicas Brasileira – ICP – Brasil.

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

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

3.3. 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.

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

3.5. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, e demais beneficiários, nos limites previstos da Lei Complementar 123/2006 e do Decreto 8.538/2015.

3.5.1. A obtenção de benefícios fica limitada às microempresas e às empresas de pequeno porte que, no ano-calendário de realização da licitação, ainda não tenham celebrado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte. **Será exigida dos licitantes declaração de observância desse limite na licitação.**

3.6. **Não poderão disputar esta licitação**:

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

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

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

3.6.4. empresas controladoras, controladas ou coligadas, nos termos da Lei 6.404/76, concorrendo entre si;

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

3.6.6. agente público de órgão ou entidade licitante ou contratante, conforme § 1º do art. 9º, da Lei 14.133/2021;

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

3.6.8. Pessoa jurídica que tenha em seu quadro societário cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade até o terceiro grau, inclusive, dos magistrados ocupantes de cargos de direção ou no exercício de funções administrativas, assim como de servidores ocupantes de cargos de direção, chefia e assessoramento, vinculados direta ou indiretamente às unidades situadas na linha hierárquica da área encarregada da licitação, conforme Resolução 07, de 18 de outubro de 2005, do Conselho Nacional de Justiça (CNJ).

3.6. O impedimento de que trata o item 3.6.2 será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

3.7. A vedação de que trata o item 3.6.6 estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

4. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

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

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

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

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

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

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

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

4.3.5. que não possui, em seu quadro societário, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, dos magistrados ocupantes de cargos de direção ou no exercício de funções administrativas, assim como de servidores ocupantes de cargos de direção ou no exercício de funções administrativas, assim como de servidores ocupantes de cargos de direção, chefia e assessoramento vinculados às unidades da área encarregada da licitação deste Tribunal, nos termos do art. 2º da Resolução nº 7/2005 do Conselho Nacional de Justiça.

4.3.6. que não possui, em seu quadro funcional, cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de ocupantes de cargos de direção e assessoramento, bem como de magistrados vinculados a este Tribunal.

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

4.5. O fornecedor enquadrado como microempresa, empresa de pequeno porte ou sociedade cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 3°, da Lei Complementar 123/2006, 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 14.133/2021.

4.5.1. no item exclusivo para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame, para aquele item;

4.5.2. nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar 123/2006, mesmo que microempresa, empresa de pequeno porte ou sociedade cooperativa.

4.6. A falsidade da declaração de que trata os itens 4.4 ou 4.5 sujeitará o licitante às sanções previstas na Lei 14.133/2021 e neste Edital.

4.7. 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.

4.8. 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.

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

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

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

4.10. O valor final mínimo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:

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

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

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

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

5. DO PREENCHIMENTO DA PROPOSTA

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

5.1.1. **Valor unitário e total de cada item pertencente a a seu respectivo Grupo**;

5.1.2. **Descrição do objeto**, contendo as informações similares à especificação do Termo de Referência*;*

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

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

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

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

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

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

5.8. A apresentação da proposta implica obrigatoriedade do cumprimento das disposições nela 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.

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

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

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

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

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

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

6.2.1. Será desclassificada a proposta que identifique o licitante.

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

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

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

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

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

6.6. **O lance deverá ser ofertado pelo valor de cada item pertencente a cada Grupo** ;

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

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

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

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

6.11. Será adotado para o envio de lances o **modo de disputa "aberto e fechado"**, em que os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

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

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

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

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

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

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

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

6.14. 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.

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

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

6.17. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de

maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45, da Lei Complementar 123/2006, regulamentada pelo Decreto 8.538/2015.

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

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

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

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

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

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

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

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

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

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

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

6.18.2.1. empresas brasileiras;

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

6.18.2.3. empresas que comprovem a prática de mitigação, nos termos da Lei 12.187/2009.

6.18.3. Esgotados todos os demais critérios de desempate previstos em lei, a escolha do licitante vencedor ocorrerá por sorteio, em ato público, no sistema Compras.gov.br, das propostas empatadas, vedado qualquer outro processo.

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

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

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

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

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

6.19.4.1. A proposta ajustada deverá conter a descrição do objeto e apresentar as informações similares à especificação do Termo de Referência.

6.19.4.2. **Conforme disposto no Acórdão/TCU 2569/2018-Plenário, deverá ser apresentada, juntamente com a proposta ajustada, declaração que ateste que a empresa não pratica registro de oportunidade junto ao fabricante do software. Se a declaração não for entregue concomitantemente à proposta, o pregoeiro fixará prazo para a sua apresentação.**

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

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

7. DA FASE DE JULGAMENTO

7.1. **Encerrada a etapa de negociação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame**, conforme previsto no art. 14 da Lei 14.133/2021, legislação correlata e no subitem 3.6 do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

7.1.1. Sistema de Cadastramento Unificado de Fornecedores – SICAF;

7.1.2. Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria Geral da União, disponível em https://www.portaltransparencia.gov.br/sancoes/ceis.

7.1.3. Certidão Negativa de Improbidade Administrativa e Inelegibilidade - CNIAI, constante do Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa, disponível no Portal do Conselho Nacional de Justiça, em http://www.cnj.jus.br/improbidade_adm/consultar_requerido.php **ou** https://certidoes-apf.apps.tcu.gov.br.

7.1.4. Lista de Inidôneos, mantida pelo Tribunal de Contas da União - TCU, disponível em https://contas.tcu.gov.br/ords/f?p=INABILITADO:CERTIDAO:0: **ou** https://certidoes-apf.apps.tcu.gov.br.

7.1.5. Cadastro Nacional de Empresas Punidas - CNEP, mantido pela Controladoria-Geral da União, disponível em https://www.portaltransparencia.gov.br/sancoes/cnep.

7.2. A consulta aos cadastros dos itens 7.1.2 ao 7.1.5 será realizada em nome da empresa licitante e também de seu(s) sócio(s) majoritário(s), por força da vedação de que trata o art. 12

da Lei 9.429/92.

7.3. Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o Pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas (IN 3/2018, art. 29, *caput*).

7.3.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros. (IN 3/2018, art. 29, § 1º).

7.3.2. O licitante será convocado para manifestação previamente a uma eventual desclassificação. (IN 3/2018, art. 29, § 2º).

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

7.4. 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 os itens 3.5.1 e 4.5 deste edital.

7.5. **Verificadas as condições de participação, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos**, observado o disposto nos artigos 29 a 35 da IN SEGES 73/2022.

7.6. **Será desclassificada a proposta vencedora que**:

7.6.1. contiver vícios insanáveis;

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

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

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

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

7.7. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências para aferir a exequibilidade das propostas ou exigir dos licitantes que ela seja demonstrada.

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

7.9. Será realizada consulta ao Cadastro Informativo de Créditos não Quitados (CADIN). Caso conste no resultado da consulta que a empresa possui registro no CADIN, a licitante será convocada a regularizar, em vista da restrição do Art. 6º-A da Lei nº 10.522/2022, ou, se for o caso, apresentar justificativas. **Porém, a irregularidade não gera impedimento para participação da licitação, mas sim para a celebração do contrato."**

8. DA FASE DE HABILITAÇÃO

8.1. Os documentos previstos ns itens 4.2.1 ao 4.2.4.5 do Termo de Referência, necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, **serão exigidos para fins de habilitação**, nos termos dos artigos 62 a 70 da Lei 14.133/2021.

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

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

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

8.3. Em caso de formação de consórcio de empresas, a habilitação técnica, quando exigida, será feita por meio do somatório dos quantitativos de cada consorciado e, para efeito de habilitação econômico-financeira, quando exigida, será observado o somatório dos valores de cada consorciado.

8.3.1. Se o consórcio não for formado integralmente por microempresas ou empresas de pequeno porte e o termo de referência exigir requisitos de habilitação econômico-financeira, haverá um acréscimo de 10%, para o consórcio em relação ao valor exigido para os licitantes individuais.

8.4. Os documentos exigidos para fins de habilitação poderão ser substituídos por registro cadastral emitido por órgão ou entidade pública, desde que o registro tenha sido feito em obediência ao disposto na Lei 14.133/2021.

8.5. Será verificado se o licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei (art. 63, I, da Lei 14.133/2021).

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

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

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

8.9. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir. (IN 3/2018, art. 4º, § 1º, e art. 6º, § 4º).

8.10. É de responsabilidade do licitante conferir a exatidão dos seus dados cadastrais no Sicaf e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados. (IN 3/2018, art. 7º, *caput*).

8.10.1. A não observância do disposto no subitem anterior poderá ensejar desclassificação no momento da habilitação. (IN 3/2018, art. 7º, parágrafo único).

8.11. A verificação pelo pregoeiro, em sítios eletrônicos oficiais de órgãos e entidades emissoras de certidões constitui meio legal de prova, para fins de habilitação.

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

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

8.12. A verificação no Sicaf ou a exigência dos documentos nele não contidos somente será feita em relação ao licitante vencedor.

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

8.13. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência (Lei 14.133/21, art. 64, e IN 73/2022, art. 39, §4º), para:

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

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

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

8.15. Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital, observado o prazo disposto no subitem 8.11.1.

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

8.17. A comprovação de regularidade fiscal e trabalhista das microempresas e das empresas de pequeno porte somente será exigida para efeito de contratação, e não como condição para participação na licitação (art. 4º do Decreto nº 8.538/2015).

9. DA ATA DE REGISTRO DE PREÇOS

9.1. Homologado o resultado da licitação, o licitante mais bem classificado terá o prazo de 5 (cinco) dias úteis, contados a partir da data de sua convocação, para assinar a Ata de Registro de Preços, cujo prazo de validade encontra-se nela fixado, sob pena de decadência do direito à contratação, sem prejuízo das sanções previstas na Lei 14.133/2021.

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

(a) a solicitação seja devidamente justificada e apresentada dentro do prazo;

(b) a justificativa apresentada seja aceita pela Administração.

9.3. A Ata de Registro de Preços será assinada por meio de assinatura digital e disponibilizada no portal Sistema de Compras do Governo Federal (www.gov.br/compras).

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

9.5. O preço registrado, com a indicação dos fornecedores, será divulgado no PNCP e disponibilizado durante a vigência da Ata de Registro de Preços.

9.6. A existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas, mas não obrigará a Administração a contratar, facultada a realização de licitação específica para a aquisição pretendida, desde que devidamente justificada (art. 21, do Decreto 11.462/2023).

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

10. DA FORMAÇÃO DO CADASTRO DE RESERVA

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

10.1.1. dos licitantes que aceitarem cotar o objeto com preço igual ao do adjudicatário, observada a classificação na licitação;

10.1.2. dos licitantes que mantiverem sua proposta original.

10.2. Será respeitada, nas contratações, a ordem de classificação dos licitantes ou fornecedores registrados na ata, conforme art. 18, III, do Decreto 11.462/2023.

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

10.2.2. Para fins da ordem de classificação, os licitantes ou fornecedores que aceitarem cotar o objeto com preço igual ao do adjudicatário antecederão aqueles que mantiverem sua proposta original (art. 18, § 2º, do Decreto 11.462/2023).

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

10.3.1. quando o licitante vencedor não assinar a Ata de Registro de Preços no prazo e nas condições estabelecidos no edital; ou

10.3.2. quando houver o cancelamento do registro do fornecedor ou do registro de preços, nas hipóteses previstas nos art. 28 e art. 29 do Decreto nº 11.462/2023.

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

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

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

11. DOS RECURSOS

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

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

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

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

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

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

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

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

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

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

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

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

12. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

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

12.1.1. Deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo/a pregoeiro/a durante o certame;

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

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

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

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

12.1.2.4. deixar de apresentar amostra;

12.1.2.4. apresentar proposta em desacordo com as especificações do edital.

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

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

12.1.4. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação.

12.1.5. Fraudar a licitação.

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

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

12.1.6.2. induzir deliberadamente a erro no julgamento;

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

12.1.8. Praticar ato lesivo previsto no art. 5º da Lei 12.846/2013.

12.2. Com fulcro na Lei 14.133/2021, a Administração poderá, garantida a prévia defesa, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

12.2.1. advertência;

12.2.2. multa;

12.2.3. impedimento de licitar e contratar;

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

12.3. Na aplicação das sanções serão considerados:

12.3.1. a natureza e a gravidade da infração cometida;

12.3.2. as peculiaridades do caso concreto;

12.3.3. as circunstâncias agravantes ou atenuantes;

12.3.4. os danos que dela provierem para a Administração Pública;

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

12.4.A multa será recolhida em percentual de 0,5% a 30% incidente sobre o valor do contrato licitado, recolhida no prazo máximo de 20 dias úteis, a contar da comunicação oficial.

12.4.1. Para as infrações previstas nos subitens 12.1.1 ao 12.1.3, a multa será de 0,5% a 15% (cinco décimos a quinze por cento) do valor do contrato licitado.

12.4.2. Para as infrações previstas nos subitens 12.1.4 ao 12.1.8, a multa será de 15% a 30% (quinze a trinta por cento) do valor do contrato licitado.

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

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

12.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos subitens 12.1.1 ao 12.1.3, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta da União, pelo prazo máximo de 3 (três) anos.

12.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos subitens 12.1.4 ao 12.1.8, bem como pelas infrações administrativas previstas nos subitens 12.1.1 ao 12.1.3 que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, § 5º, da Lei 14.133/2021.

12.9. A recusa injustificada do adjudicatário em assinar o contrato ou a Ata de Registro de Preços, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no subitem 12.1.3, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação, nos termos do art. 45, § 4º da IN SEGES/ME 73/2022.

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

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

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

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

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

13. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

13.1. Qualquer pessoa é parte legítima para impugnar este Edital por irregularidade na aplicação da Lei 14.133/2021, devendo protocolar o pedido até 3 (três) dias úteis antes da data da abertura do certame.

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

13.3. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica, por envio de e-mail ao endereço licitacao.mg@trf6.jus.br.

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

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

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

14. DAS DISPOSIÇÕES GERAIS

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

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

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

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

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

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

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

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

14.9. Em caso de divergência entre as descrições no Comprasnet (especialmente códigos CATMAT/CATSER) e as disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

14.10. O Edital e seus anexos estão disponíveis, na íntegra, no **Portal Nacional de Contratações Públicas (PNCP), e no** endereço eletrônico **https://portal.trf6.jus.br/institucional/compras-e-licitacoes/ - link "Licitações do TRF6/SJMG a partir de 19/08/2022"**.

14.11. Outros esclarecimentos sobre a presente licitação poderão ser obtidos em dias úteis, por meio do e-mail licitacao@trf6.jus.br.

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

. TERMO DE REFERÊNCIA

ANEXO I - Especificações

. **CLASSIFICAÇÃO ORÇAMENTÁRIA**

. ESTUDO TÉCNICO PRELIMINAR

. MINUTA DA ATA DE REGISTRO DE PREÇOS

. MINUTA DO CONTRATO

Eloísa Cruz Moreira de Carvalho

Diretora da Secretaria de Orçamento, Finanças e Contratações - SECOF

- assinado eletronicamente -

Documento assinado eletronicamente por **Eloisa Cruz Moreira de Carvalho**, **Diretor(a) de Secretaria**, em 21/02/2025, às 15:20, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

PODER JUDICIÁRIO
TRIBUNAL REGIONAL FEDERAL DA 6ª REGIÃO
Subsecretaria de Infraestrutura

TERMO DE REFERÊNCIA

1. OBJETO

1.1. Definição do objeto

1.1.1. Registrar preços para eventual aquisição de Solução de Segurança de TIC com a finalidade de atender às necessidades de funcionamento dos sistemas do Tribunal Regional Federal da 6ª Região

1.2. Descrição detalhada do objeto

1.2.1. Aquisição de Solução de Segurança de TIC, incluindo o fornecimento de appliances de NGFW e respectivos licenciamentos, o licenciamento de Appliance Virtual de Web Application Firewall e o licenciamento de Serviço de Segurança de Borda (Security Service Edge - SSE), incluindo os serviços de instalação, suporte técnico e treinamento, por um período de 60 (sessenta) meses.

1.2.1.1. Para o ÓRGÃO GERENCIADOR, conforme itens e quantidades abaixo:

LOTES	ITENS	CATMAT / CATSER	SERVIÇOS	UNIDADES REFERENCIAIS	QUANTIDADES
01 TRF6	01	484747	Appliances de Next Generation Firewall	Unidade	2
	02	27472	Licenciamentos para operações de Next Generation Firewall por 60 meses	Conjunto	1
	03	26972	Instalação e Configuração	Conjunto	1
	04	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60
	05	3840	Treinamento	Turma	1
02 TRF6	06	27472	Web Application Firewall - Appliance Virtual	Unidade	1
	07	26972	Instalação e Configuração	Conjunto	1
	08	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60
	09	3840	Treinamento	Turma	1
03 TRF6	10	27472	Serviço de Segurança de Borda (Security Service Edge - SSE)	Usuários	4.500
	11	26972	Instalação e Configuração	Conjunto	1
	12	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60
	13	3840	Treinamento	Turma	1

1.2.1.2. Para os ÓRGÃOS PARTICIPANTES, conforme itens e quantidades abaixo:

1.2.1.2.1. Justiça Federal da 4ª Região:

LOTES	ITENS	CATMAT / CATSER	SERVIÇOS	UNIDADES REFERENCIAIS	QUANTIDADES
04 TRF4	10	27472	Serviço de Segurança de Borda (Security Service Edge - SSE)	Usuários	1.250
	11	26972	Instalação e Configuração	Conjunto	1
	12	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60
	13	3840	Treinamento	Turma	1
05 SJPR	10	27472	Serviço de Segurança de Borda (Security Service Edge - SSE)	Usuários	2.500
	11	26972	Instalação e Configuração	Conjunto	1
	12	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60
	13	3840	Treinamento	Turma	1
06 SJRS	10	27472	Serviço de Segurança de Borda (Security Service Edge - SSE)	Usuários	150
	11	26972	Instalação e Configuração	Conjunto	1
	12	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60
	13	3840	Treinamento	Turma	1
	10	27472	Serviço de Segurança de Borda (Security Service Edge - SSE)	Usuários	1.450

07 SJSC	11	26972	Instalação e Configuração	Conjunto	1
	12	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60
	13	3840	Treinamento	Turma	1

1.2.1.2.2. Justiça Federal da 5ª Região:

LOTES	ITENS	CATMAT / CATSER	SERVIÇOS	UNIDADES REFERENCIAIS	QUANTIDADES
08 SJCE	10	27472	Serviço de Segurança de Borda (Security Service Edge - SSE)	Usuários	1.400
	11	26972	Instalação e Configuração	Conjunto	1
	12	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60
	13	3840	Treinamento	Turma	1
09 SJRN	10	27472	Serviço de Segurança de Borda (Security Service Edge - SSE)	Usuários	1.000
	11	26972	Instalação e Configuração	Conjunto	1
	12	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60
	13	3840	Treinamento	Turma	1
10 SJSE	10	27472	Serviço de Segurança de Borda (Security Service Edge - SSE)	Usuários	400
	11	26972	Instalação e Configuração	Conjunto	1
	12	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60
	13	3840	Treinamento	Turma	1

1.2.2. O objeto da licitação tem natureza de serviço comum de Tecnologia da Informação, por apresentar, independentemente de sua complexidade, “padrões de desempenho e qualidade que possam ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado”.

1.3. A contratação será na modalidade Pregão Eletrônico através de sistema de registro de preços - Pregão Eletrônico - Menor Preço, com fundamento nos seguintes normativos:

1.3.1. Lei nº 14.133, de 1º de abril de 2021, que dispõe sobre as normas para licitações e contratos administrativos;

1.3.2. Decreto nº 11.462, de 31 de março de 2023, que regulamenta os art. 82 a art. 86 da Lei nº 14.133, de 1º de abril de 2021, para dispor sobre o sistema de registro de preços para a contratação de bens e serviços, inclusive obras e serviços de engenharia, no âmbito da Administração Pública federal direta, autárquica e fundacional;

1.3.3. Plano Estratégico de Tecnologia da Informação da Justiça Federal - PETI 2021/2026, aprovado pela Resolução CJF n. 685/2020;

1.3.4. Resolução CNJ 370/2021, que estabelece a Estratégia Nacional de Tecnologia da Informação do Poder Judiciário (ENTIC-JUD) para o período 2021/2026;

1.3.5. Resolução CNJ 468/2022, dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça (CNJ).

1.4. O contrato entra em vigor a partir da data de assinatura. O fim da vigência do contrato será fixada por apostilamento, após o recebimento definitivo do objeto, contando-se 60 (sessenta) meses a partir deste marco, que deverá ser certificado no processo pelo gestor designado.

1.4.1. A vigência indicada é justificada pelas nuances da contratação e de seu objeto e pelo esforço inicial exigido para a implantação das ferramentas envolvidas na prestação dos serviços, assim como a continuidade da operação dos serviços e sistemas.

1.4.2. A prorrogação contratual pressupõe anuência do CONTRATANTE e da CONTRATADA, demonstrada a manutenção da vantagem para o CONTRATANTE das condições contratadas e do preço praticado.

1.4.3. A falta de interesse na prorrogação contratual deverá ser manifestada expressamente pela CONTRATADA em até 180 (cento e oitenta) dias antes do encerramento da vigência do contrato, independentemente de provocação pelo CONTRATANTE, com vistas a viabilizar um novo procedimento licitatório.

2. JUSTIFICATIVA, FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

A atual infraestrutura de TIC que atende ao TRF6 foi preparada para o funcionamento de uma Seccional, razão pela qual o recebimento de sistemas anteriormente centralizados no TRF1 como o PJe, o SEI, Acordo 58, SIREA, eSiest, bancos de dados, entre outros, representou um consumo de recursos não previstos quando das aquisições, conforme cenário de escassez reportado por meio dos autos 0000724-85.2022.4.06.8000.

Diante do crescimento dos sistemas do TRF6, inúmeras aplicações anteriormente hospedadas no TRF1 passaram a ser publicadas na internet, o que representou o estabelecimento de um tráfego de conexões não dimensionado para a SJMG. Assim, a atual solução de segurança se mostrou insuficiente face à demanda cada vez maior de acessos, incluindo as vias automatizadas por robôs.

Destaca-se que as appliances de firewall Check Point 13500 alcançaram o chamado fim de utilização em junho de 2022 (vide relato do fabricante), o que obrigou a migração das operações para um modelo Open Server no ano

de 2022, conforme Segundo Termo Aditivo ao Contrato n. 0035/2020 do TRF1 (Documento SEI TRF1 16656397).

Uma solução de segurança possui uma garantia recomendada de 04 anos com posterior substituição após a vigência, nos termos da Resolução CJF nº 477/2018, em razão da obsolescência técnica dos equipamentos. Por tal razão e considerando que os firewalls do TRF6 possuem mais de 8 anos de uso, além de não atenderem à atual demanda técnico-operacional, torna-se necessária a substituição dos equipamentos para adequação às necessidades de funcionamento do TRF6.

Outro ponto a se destacar é a dificuldade de tratamento dos acessos aos sistemas, em razão da indisponibilidade de WAF. Assim, os sistemas do TRF6 dependem de configurações individualizadas para o controle dos acessos automatizados frequentemente realizados por meio de robôs e bots, alguns dos quais de caracteres maliciosos.

Há, ainda, um elemento essencial à infraestrutura: a disponibilidade. Todos os sistemas do TRF6 devem estar disponíveis para funcionamento em regime de 24 x 7 (vinte e quatro horas, sete dias por semana), o que pode acarretar em situações de falhas em horários sem acompanhamento por equipe especializada e, consequentemente, em atraso para o início do atendimento. Considerando que os sistemas e serviços de TI do TRF6 sustentam a área finalística da instituição, torna-se cada vez mais importante que estejam hospedados em ambiente de infraestrutura tecnológica protegida e que garanta a disponibilidade e integridade das informações.

A contratação visa a adquirir uma solução de segurança de alta complexidade diante da necessidade de implantação aderente à LGDP, em substituição ao atual sistema obsoleto de proteção de perímetro de rede com a inclusão de novas funcionalidades de proteção de rede que compõem a plataforma de segurança de nova geração. A nova solução incluirá recursos de reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões, sistemas de detecção de invasão e sistemas de prevenção de intrusão, aplicações antimalware, inspeção de pacotes SSL/TLS, já que o tráfego é frequentemente criptografado para evitar a detecção e bloqueio de ameaças. Também permitirá o combate à falsificação de tráfego de acesso, o que dificulta a identificação e o bloqueio com base em assinaturas ou padrões específicos em razão do caráter aparentemente legítimo, ao parque tecnológico do TRF6.

Por tudo exposto, busca-se com a presente contratação:

- Atualizar o parque tecnológico do TRF6;
- Obter serviços de alta disponibilidade;
- Aumentar a velocidade de operação entre os equipamentos;
- Otimizar o desempenho da rede de dados;
- Garantir a estabilidade operacional das comunicações do TRF6 e suas subseções judiciárias;
- Aumentar a proteção de rede do TRF6, possibilitando a inspeção de tráfego com maior granularidade que a atualmente realizada;
- Melhorar o desempenho e eficácia no controle de acesso ao perímetro de rede através de equipamentos com níveis de processamento e capacidade mais adequados;
- Aumentar a disponibilidade das aplicações, evitando o comprometimento da capacidade do firewall em eventuais situações de ataque;
- Possuir viabilidade para realizar futuras expansões da capacidade e granularidade da rede do Tribunal;
- Possibilitar a ampliação da segmentação da rede com o objetivo de reduzir os riscos de segurança;
- Aumento da resiliência em caso de ataques;
- Diminuir o tempo de análise e resolução de problemas.

3. ALINHAMENTO ESTRATÉGICO

- Resolução CNJ nº 370, de 28 de janeiro de 2021 - Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);
- Resolução CJF nº 685, de 15 de dezembro de 2020 - Plano Estratégico de Tecnologia da Informação da Justiça Federal.

Macrodesafio: Fortalecimento da Estratégia Nacional de TIC e de Proteção de Dados

Objetivos Estratégicos da Justiça Federal:

1) Aperfeiçoar e assegurar a efetividade dos serviços de TI para a Justiça Federal.

Indicadores	Metas
1 - Índice de satisfação dos clientes internos com os serviços de TI.	1 - Atingir, até 2025, 85% de satisfação dos clientes internos de TI.
2 - Índice de satisfação dos clientes externos com os serviços de TI.	2 - Atingir, até 2026, 80% de satisfação dos clientes externos de TI.

4. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

4.1. Forma de seleção e critério de julgamento da proposta

4.1.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo **MENOR PREÇO**.

4.2. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

4.2.1. Habilitação técnica

4.2.1.1. Comprovação através de atestado de capacidade técnica, no mínimo, 01 (um), para cada lote descrito no edital**,** em nome da licitante**,** fornecido por pessoa jurídica de direito público ou privado, e que comprove que:

4.2.1.1.1. A prestadora executou, diretamente, serviços compatíveis com aqueles exigidos por este Termo de Referência, sendo: instalação, customização, suporte, treinamento e operação assistida.

4.2.1.2. A licitante deverá ser revenda autorizada a realizar o fornecimento de produtos e serviços pelo fabricante da solução;

4.2.1.2.1. As soluções de cybersegurança utilizam equipamentos e funcionalidades de altas complexidades tecnológicas, razão pela qual qualquer mínimo problema ou má configuração pode gerar a parada total dos serviços e sistemas essenciais ao funcionamento do Tribunal;

4.2.1.2.2. A exigência quanto ao licitante integrar a lista de *global partners* se deve ao respaldo dos fabricantes quanto à origem, controle, garantia e suporte, entre outros elementos.

4.2.1.3. Para verificar a autenticidade dos atestados apresentados, a CONTRATANTE poderá realizar diligências ou requerer os comprovantes fiscais da execução do objeto;

4.2.1.4. A CONTRATANTE se reserva o direito de realizar diligências para apuração da veracidade dos serviços/produtos de que trata(m) o(s) atestado(s).

4.2.2. Habilitação jurídica

4.2.2.1. Pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

4.2.2.2. Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede; Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-enegocios/pt-br/empreendedor;

4.2.2.3. 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;

4.2.2.4. 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, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020;

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

4.2.2.6. 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;

4.2.2.7. Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971;

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

4.2.3. Habilitação fiscal, social e trabalhista

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

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

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

4.2.3.4. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa;

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

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

4.2.3.7. Caso o fornecedor seja considerado isento dos tributos relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei;

4.2.3.8. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal;

4.2.4. Qualificação Econômico-Financeira

4.2.4.1. Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante,

caso se trate de pessoa física, desde que admitida a sua participação na licitação ou de sociedade simples;

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

4.2.4.3. 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:

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

II - Solvência Geral (SG)= (Ativo Total) / (Passivo Circulante +Passivo não Circulante); e

III - Liquidez Corrente (LC) = (Ativo Circulante) / (Passivo Circulante).

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

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

5. DETALHAMENTO DOS LOTES E ITENS

5.1. Segue abaixo a descrição dos lotes, itens e quantitativos a serem contratados:

5.1.1. Para o ÓRGÃO GERENCIADOR, conforme itens e quantidades abaixo:

LOTES	ITENS	CATMAT / CATSER	SERVIÇOS	UNIDADES REFERENCIAIS	QUANTIDADES
01 TRF6	01	484747	Appliances de Next Generation Firewall	Unidade	2
	02	27472	Licenciamentos para operações de Next Generation Firewall por 60 meses	Conjunto	1
	03	26972	Instalação e Configuração	Conjunto	1
	04	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60
	05	3840	Treinamento	Turma	1
02 TRF6	06	27472	Web Application Firewall - Appliance Virtual	Unidade	1
	07	26972	Instalação e Configuração	Conjunto	1
	08	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60
	09	3840	Treinamento	Turma	1
03 TRF6	10	27472	Serviço de Segurança de Borda (Security Service Edge - SSE)	Usuários	4.500
	11	26972	Instalação e Configuração	Conjunto	1
	12	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60
	13	3840	Treinamento	Turma	1

5.1.2. Para os ÓRGÃOS PARTICIPANTES, conforme itens e quantidades abaixo:

5.1.2.1. Justiça Federal da 4ª Região:

LOTES	ITENS	CATMAT / CATSER	SERVIÇOS	UNIDADES REFERENCIAIS	QUANTIDADES
04 TRF4	10	27472	Serviço de Segurança de Borda (Security Service Edge - SSE)	Usuários	1.250
	11	26972	Instalação e Configuração	Conjunto	1
	12	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60
	13	3840	Treinamento	Turma	1
05 SJPR	10	27472	Serviço de Segurança de Borda (Security Service Edge - SSE)	Usuários	2.500
	11	26972	Instalação e Configuração	Conjunto	1
	12	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60
	13	3840	Treinamento	Turma	1

06 SJRS	10	27472	Serviço de Segurança de Borda (Security Service Edge - SSE)	Usuários	150
	11	26972	Instalação e Configuração	Conjunto	1
	12	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60
	13	3840	Treinamento	Turma	1
07 SJSC	10	27472	Serviço de Segurança de Borda (Security Service Edge - SSE)	Usuários	1.450
	11	26972	Instalação e Configuração	Conjunto	1
	12	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60
	13	3840	Treinamento	Turma	1

5.1.2.2. Justiça Federal da 5ª Região:

LOTES	ITENS	CATMAT / CATSER	SERVIÇOS	UNIDADES REFERENCIAIS	QUANTIDADES
08 SJCE	10	27472	Serviço de Segurança de Borda (Security Service Edge - SSE)	Usuários	1.400
	11	26972	Instalação e Configuração	Conjunto	1
	12	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60
	13	3840	Treinamento	Turma	1
09 SJRN	10	27472	Serviço de Segurança de Borda (Security Service Edge - SSE)	Usuários	1.000
	11	26972	Instalação e Configuração	Conjunto	1
	12	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60
	13	3840	Treinamento	Turma	1
10 SJSE	10	27472	Serviço de Segurança de Borda (Security Service Edge - SSE)	Usuários	400
	11	26972	Instalação e Configuração	Conjunto	1
	12	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60
	13	3840	Treinamento	Turma	1

5.1.1. Em caso de discordância existente entre as especificações descritas no Comprasnet (código BR) e as especificações técnicas constantes deste instrumento, prevalecerão as deste instrumento.

5.1.2. Todos os itens dos lotes da presente contratação são interdependentes entre si, razão pela qual a adjudicação DEVERÁ ser realizada por LOTES.

5.2. JUSTIFICATIVAS DAS QUANTIDADES

5.2.1. Para o lote 1, a quantidade representa o mínimo necessário para a garantia de alta disponibilidade;

5.2.1.1. O item 2 corresponde aos licenciamentos das funcionalidades de Next Generation Firewall, razão pela qual é necessário todo o conjunto correspondente aos recursos;

5.2.2. O item 6 corresponde a um licenciamento com possibilidade de utilização em ambientes on premises ou em nuvem;

5.2.3. O item 10 trata de licenciamento por usuário do serviço. Considerando que o TRF6 e suas subseções judiciárias possuem atualmente aproximadamente 4.000 usuários, estima-se um crescimento de 10% ao longo dos 60 (sessenta) meses de vigência contratual;

5.2.4. Os itens 3, 7 e 11 correspondem aos serviços de instalação e configuração dos lotes 1 a 3, portanto de execução imediata;

5.2.6. Os itens 4, 8 e 12 tratam dos suportes técnicos dos lotes e serão faturados mensalmente.

5.2.7. Por fim, os itens 5, 9 e 13 correspondem às turmas de treinamentos referente aos lotes, portanto de execução imediata;

5.2.7.1. Os treinamentos serão realizados para turmas de 10 (dez) alunos.

6. REQUISITOS DA CONTRATAÇÃO

6.1. Requisitos de Negócio

6.1.1. Assegurar a efetividade dos serviços de TI para o TRF6, através da continuidade dos serviços de

segurança de dados e aplicações e de proteção contra ameaças;

6.1.2. Assegurar a proteção dos dados dos sistemas e dos usuários do TRF6 de acordo com a Política de Segurança da Informação do CJF, aplicável em razão da falta de norma própria;

6.1.3. As especificações dos equipamentos, licenciamentos e serviços se encontram definidas no Anexo I - Especificações deste Termo de Referência.

6.2. Requisitos de Garantia

6.2.1. A garantia da solução deve permitir reparar eventuais falhas e substituir peças com defeito por outras de configuração idêntica ou superior;

6.2.2. A garantia da solução deve permitir a atualização dos produtos licenciados assim que novas versões e releases dos softwares que fizerem parte da solução contratada estiverem disponíveis.

6.3. Requisitos Técnicos

6.3.1. Os serviços de suporte deverão ser capazes de atender às demandas de compatibilidade da solução de segurança com a infraestrutura computacional existente no TRF6.

6.3.2. As especificações dos itens

6.4. Requisitos de Suporte

6.4.1. Será prestado serviço de suporte técnico durante toda a vigência do contrato, com direito a atualizações de versões da solução que incorporem correções de defeitos e melhorias implementadas pelos fabricantes.

6.5. Requisitos de Manutenção

6.5.1. A solução proposta deverá possuir garantia do fabricante de 05 anos para entrega de peças on-site;

6.5.2. Atendimento 24x7 nas dependências do TRF6;

6.5.3. Substituir componentes e peças defeituosos ou com falhas, trocas periódicas das peças internas, discos e demais componentes que apresentarem problemas técnicos durante a vigência do contrato, utilizando de produtos originais, novos e de primeiro uso, garantidos pelo fabricante;

6.5.4. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos no processo de contratação, com observância às recomendações aceitas pela boa técnica, normas e legislação, bem como observar conduta adequada na utilização dos materiais, equipamentos, ferramentas e utensílios;

6.5.5. Possibilitar o suporte técnico e especializado, remoto ou presencial, entre o CONTRATANTE e o fabricante sem novos ônus ou custos contratuais;

6.5.6. Executar todas as atividades de instalação, atualização, configuração e migração de acordo com o planejamento aprovado pela área técnica;

6.5.7. Realizar manutenção corretiva, que compreende providências para reparar e corrigir os componentes da solução contratada em seu pleno estado de funcionamento, removendo definitivamente os defeitos eventualmente apresentados;

6.5.8. Garantir o funcionamento do ambiente com relação à solução instalada pela CONTRATADA, incluindo todos os serviços necessários para manutenção da disponibilidade da solução, inclusive de configurações e fornecimento de “firmwares”, “fixes” e “releases”, durante toda a vigência do contrato;

6.5.9. Os serviços serão solicitados mediante a abertura de um chamado efetuado por técnicos da contratante, via chamada telefônica local, a cobrar ou 0800, e-mail, website ou chat do fabricante ou à empresa autorizada (em português – para o horário comercial – horário oficial de Brasília) e constatada a necessidade, o fornecedor deverá providenciar o deslocamento do equipamento, bem como seu retorno ao local de origem sem qualquer ônus ao contratante.

6.6.6. Requisitos de Instalação

6.6.1. A realização dos serviços deve ser planejada de acordo com disponibilidade de ambas as partes. O planejamento anterior ao serviço deverá ser realizado de forma on-site nas dependências da CONTRATANTE;

6.6.2. O planejamento dos serviços de instalação deve resultar num documento tipo SOW (em tradução livre, escopo de trabalho). Neste documento devem conter a relação, descrição e quantidades dos produtos fornecidos, descrição da infraestrutura atual e desejada, detalhamento dos serviços que serão executados, premissas do projeto, locais e horários de execução dos serviços, condições de execução dos serviços, pontos de contato da CONTRATADA e CONTRATANTE, cronograma de execução do projeto em etapas, com responsáveis e data e início e fim (se aplicável), relação da documentação a ser entregue ao final da execução dos serviços, responsabilidade da CONTRATADA, plano de gerenciamento de mudanças, itens excluídos no projeto e termo de aceite. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes;

6.6.3. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, devendo a CONTRATADA sugerir as configurações de acordo com normas técnicas e boas práticas, cabendo à CONTRATANTE a sua aceitação expressa ou recusa nos casos de não atendimento das condições estabelecidas;

6.6.4. Após a instalação, a solução deverá ser monitorada on-site nas dependências da CONTRATANTE pelo prazo mínimo de 8 (oito) horas corridas, observando as condições de funcionamento e performance dos equipamentos, sendo possível o troubleshooting em caso de problemas ou não conformidades na operação;

6.6.5. Ao final da instalação, deverá ser realizado o repasse de configurações hands-on, de forma on-site nas dependências da CONTRATANTE apresentando as configurações realizadas. A CONTRATANTE disponibilizará o local adequado para a transferência do conhecimento e acesso a solução em produção;

6.6.6. Os serviços deverão ser realizados por pessoal técnico experiente e certificado pelo fabricante da solução. Em momento anterior à instalação, a CONTRATANTE poderá solicitar os comprovantes da qualificação

profissional do(s) técnico(s) que executará(ão) os serviços, sendo direito da mesma a sua aceitação ou exigência de troca de profissional no caso de este não satisfazer às condições supramencionadas;

6.6.7. Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados no projeto (relatório as-built), etapas de execução e toda informação pertinente para posterior continuidade e manutenção da solução instalada, como usuários e endereços de acesso, configurações realizadas e o resumo das configurações dos equipamentos. Este relatório deve ser enviado com todas as informações em até 15 dias após a finalização dos serviços;

6.6.8. Nos valores cotados devem estar inclusas todas as despesas com deslocamento, alimentação e estadia para realização dos serviços (on site) nos locais de presença da CONTRATANTE. Os funcionários da CONTRATADA deverão possuir todo o ferramental necessário ao exercício das suas atividades;

6.6.9. A CONTRATADA deverá garantir a confidencialidade das informações, dados e senhas compartilhadas da CONTRATANTE;

6.6.10. A execução dos serviços ocorrerá na sede da CONTRATANTE;

6.6.11. Durante as atividades realizadas na prestação do serviço, o técnico da CONTRATADA deverá demonstrar à equipe técnica de acompanhamento da CONTRATANTE como instalar e configurar os equipamentos e os softwares fornecidos (instalação assistida);

6.6.12. As atividades deverão ser realizadas dentro do horário comercial.

6.6.7. Requisitos de Conformidade

6.7.1. Deverá fazer parte do catálogo de produtos comercializados pelo fabricante e não ter sido descontinuado;

6.7.2. Deverá ser novo, sem uso, e constar no site do fabricante (documento oficial e público) como em linha de produção;

6.7.3. Deverá permitir a utilização de todas as funcionalidades, tecnologias e recursos especificados, durante a vigência CONTRATADA, irrestrita e sem necessidade de licenciamentos ou ônus adicionais.

6.8. Requisitos Temporais

6.8.1. Apresentar plano de implantação contendo os requisitos de instalação e cronograma de entrega, instalação, configuração e disponibilização da solução, em até 30 (trinta) dias corridos da assinatura do contrato;

6.8.2. Entregar os bens e serviços no prazo máximo de até 90 (noventa) dias corridos, a contar da emissão da Ordem de Fornecimento;

6.8.3. A entrega deverá ser formalizada mediante comunicação escrita da CONTRATADA ao CONTRATANTE;

6.8.4. Executar a conferência dos produtos especificados, conjuntamente com representantes da CONTRATADA, para emissão do Termo de Recebimento Provisório;

6.8.5. Antes de findar o prazo fixado a empresa CONTRATADA poderá formalizar, de forma devidamente fundamentada, pedido de sua prorrogação, cujas razões expostas serão examinadas pela administração do CONTRATANTE, que decidirá pela prorrogação do prazo ou aplicação das penalidades previstas;

6.8.6. A CONTRATADA receberá cópia do “Termo de Recebimento Provisório” após a entrega e conferência dos produtos em até 5 (cinco) dias úteis da confirmação de entrega, contados do primeiro dia imediatamente posterior à confirmação de entrega dos itens no CONTRATANTE, desde que não haja pendências de responsabilidade da CONTRATADA;

6.8.7. Concluir, no prazo de 30 (trinta) dias corridos, a contar da emissão do termo de recebimento provisório, a implantação e configuração dos produtos, em plena compatibilidade com o ambiente computacional do CONTRATANTE e em conformidade com a proposta técnica apresentada, cumprindo ainda todas as demais cláusulas de garantia e atendimento técnico constantes do contrato, nos prazos e termos ali estipulados;

6.8.8. A CONTRATADA receberá cópia do “Termo de Recebimento Definitivo”, que deverá ser providenciado pelo CONTRATANTE no prazo máximo de 10 (dez) dias úteis, após manifestação da CONTRATADA de conclusão dos serviços e comprovação de atendimento de todas as fases, desde que a CONTRATADA atenda a todas as solicitações e que não haja pendências de sua responsabilidade;

6.8.9. Os serviços de suporte e garantia deverão estar disponíveis para atendimento durante os 07 (sete) dias corridos da semana, 24 (vinte e quatro) horas por dia;

6.8.10. Considerar o horário das 07 horas às 20 horas como de horário normal de expediente, para os dias úteis.

6.9. Requisitos de Sustentabilidade Ambiental

6.9.1. A CONTRATADA será responsabilizada por qualquer prejuízo que venha causar ao TRF6 por ter suas atividades suspensas, paralisadas ou proibidas por falta de cumprimento de normas ligadas ao software e ainda aos serviços elencados no presente Termo de Referência;

6.9.2. A CONTRATADA deverá comprovar que os produtos ofertados atendem aos critérios de segurança, compatibilidade eletromagnética e eficiência energética, previstos no art. 3º, inciso II, do Decreto n. 7.174, de 12 de maio de 2010, regulamentado pela Portaria INMETRO n. 170, de 10 de abril de 2012;

6.9.3. Só será admitida a oferta de bens de informática e/ou automação que não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr (VI)), cádmio (Cd), bifenil polibromados (PBBs), éteres difenil-polibromados (PBDEs), conforme o art. 5º, inciso IV, da IN MPOG 01, de 19 de janeiro de 2010;

6.9.4. As comprovações dos dois itens anteriores, quando exigidas pela CONTRATANTE, poderá ser feita

mediante apresentação de certificação emitida por instituição pública oficial ou instituição credenciada, ou por qualquer outro meio de prova, em especial laudo pericial, que ateste que os bens fornecidos cumprem com as exigências do edital, conforme art. 42, inciso III, da Lei 14.133, de 1º de abril de 2021;

6.9.5. A CONTRATADA deverá, para a execução do contrato, fornecer aos empregados os equipamentos de segurança que se fizerem necessários, para a execução de serviços, conforme disposto no art. 6°, inciso IV, da Instrução Normativa SLTI/MPOG n. 01, de 19 de janeiro de 2010;

6.9.6. A CONTRATADA deverá se atentar às normas em vigor atinentes à sustentabilidade expressas na 2ª edição do Manual de Sustentabilidade de compras e contratos do Conselho da Justiça Federal, instituído pela Portaria CJF n. 96, de 10 de fevereiro de 2023;

6.9.7. A CONTRATADA deverá respeitar a legislação vigente e as normas técnicas, elaboradas pela ABNT e pelo INMETRO para aferição e garantia de aplicação dos requisitos mínimos de qualidade e acessibilidade do software e ainda dos serviços elencados no Termo de Referência.

7. CONTROLE DE ACESSO E VALIDAÇÃO

7.1. A habilitação de credenciais será disponibilizada por níveis de acesso, ficando a critério do TRF6 definir os usuários que receberão contas de acesso e seus perfis de privilégios.

8. DA PROPRIEDADE INTELECTUAL E DIREITO AUTORAL

8.1. Todos os produtos advindos da execução contratual, incluindo, porém não se limitando a, documentos descritivos da solução, diagramas de conexão, “as-builts”, rotinas de migração e rotinas computacionais desenvolvidas, são de propriedade exclusiva do TRF6.

8.2. Tais produtos deverão ter tratamento confidencial por parte da CONTRATADA, que não poderá divulgá-las a terceiros sem o expresso consentimento do Tribunal.

9. NÍVEIS DE SERVIÇO

9.1. O suporte técnico deverá estar disponível, no mínimo, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, mediante e-mail ou outro sistema de abertura que permita o registro com controle de histórico;

9.2. Disponibilidade para abertura de chamado: 24x7x365 (web, e-mail ou telefone);

9.3. Disponibilidade para início de atendimento na severidade máxima: até 2h dentro do horário do suporte técnico;

9.4. O tempo de solução será contabilizado entre a abertura do chamado e restabelecimento do sistema em sua totalidade;

9.5. O tempo de atendimento inicia-se com a primeira intervenção pelo representante da Contratada, local ou remotamente;

9.6. As multas por descumprimento de prazo serão aplicadas sobre os valores mensais do suporte técnico, sem prejuízo das demais sanções previstas no Edital e Anexos;

9.7. Em caso de problema ou incidente de hardware ou de software, os seguintes prazos máximos deverão ser obedecidos para o início do atendimento e término da correção do problema:

Severidade	Descrição	Acordo de Nível de Serviço - ANS
1 (severidade máxima)	Alteração de regras e políticas de segurança	Em até 1 hora
2 (severidade máxima)	Parada total da solução - mecanismos de contingência não funcionam; indisponibilidade total ou parcial das instâncias de um cluster no sítio; indisponibilidade total de um ou mais serviços das instâncias que compõem um sítio; degradação de serviços providos pelas instâncias que compõem o sítio; indisponibilidade ou degradação no mecanismo de balanceamento entre os sítios	Em até 1 hora
3 (severidade máxima)	Alteração de configurações	Em até 1 hora e 30 minutos
4 (severidade máxima)	Verificação de problemas de desempenho e/ou disponibilidade	Em até 3 horas
5	Verificação e filtragem de logs	Em até 1 hora
6	Esclarecimento de dúvidas/revisão de regras	Em até 24 horas
7	Aqueles para os quais houver solução de contorno cujo impacto não comprometa a operação dos serviços que utilizam a solução	7 dias
8	Aqueles que não afetem o perfeito funcionamento da solução	7 dias

9.8. O descumprimento de quaisquer das obrigações assumidas importará na aplicação das seguintes glosas:

Tempo decorrido entre o primeiro apontamento de indisponibilidade e a recuperação da disponibilidade do serviço	Glosas
Até 1 hora	Sem aplicação de multa
1 a 2 horas	1% sobre o valor mensal do respectivo item

2 a 4 horas	2% sobre o valor mensal do respectivo item
4 a 8 horas	3% sobre o valor mensal do respectivo item
8 a 12 horas	4% sobre o valor mensal do respectivo item
12 a 24 horas	5% sobre o valor mensal do respectivo item
24 a 48 horas	Inexecução Parcial
Acima de 48 horas	Inexecução Total

9.8.1. Por inexecução parcial ou total do contrato, a CONTRATADA estará sujeita a glosa de 15% (quinze por cento) sobre a parte não executada, ou sobre o valor total do contrato.

9.8.2. A inexecução total ensejará a abertura de processo administrativo para apuração de responsabilidade e eventual penalização, sem prejuízo da aplicação da multa prevista no item 9.8.1.

9.9. O Serviço de Segurança de Borda obedecerá ao Acordo de Nível de Serviço (ANS) de disponibilidade abaixo detalhado:

Indicador: Disponibilidade do Serviço de Segurança de Borda (Security Service Edge - SSE)	
Descrição do Indicador	Percentual de tempo, durante o período do mês de operação, em que o serviço venha a permanecer em condições normais de funcionamento.
Fórmula de Cálculo	IDM=[(To-Ti)/To]*100 Onde: IDM = índice de disponibilidade mensal do serviço em % To = período de operação (um mês) em minutos. Ti = somatório dos tempos de inoperância durante o período de operação (um mês) em minutos. No caso de inoperância reincidente num período inferior a 3 (três) horas, contado a partir do restabelecimento do enlace da última inoperância, considerar-se-á como tempo de indisponibilidade do enlace o início da primeira inoperância até o final da última inoperância, quando o enlace estiver totalmente operacional. A indisponibilidade de dados de gerência (coleta não realizada, dados não acessíveis, etc.) será considerada como indisponibilidade do serviço, caso isto implique em perda de dados de gerenciamento. Os tempos de inoperância serão os tempos em que os enlaces apresentarem problemas que serão obtidos dos chamados abertos no sistema de abertura de chamados técnicos (Trouble Ticket) e os tempos de indisponibilidade computados pela violação do indicador de retardo. Somente serão desconsiderados os tempos de inoperância, causados por manutenções programadas com o TRF6, ressalvados, contudo, os casos fortuitos e de força maior.
Periodicidade de Aferição	Mensal
Limiar de Qualidade	Disponibilidade mensal mínima (em %): 99,7%
Pontos de Controle	A CONTRATADA realizará, por meio da solução de gerenciamento, a coleta e o armazenamento de informações a respeito de todos os enlaces pelo tempo de duração do contrato.
Relatórios de Níveis de Serviço (RNS)	A CONTRATADA deverá disponibilizar mensalmente ao TRF6 os relatórios com os índices apurados diariamente, totalizados e apresentados mensalmente pelo serviço. A CONTRATADA deverá disponibilizar relatório analítico com os tempos de falhas (com hora de início e fim da inoperância) e minutos excedentes ao prazo máximo para reparo e disponibilidade no período (mês).
Glosa no caso de Inadimplemento	0,5% (meio por cento) por décimo porcentual de disponibilidade abaixo do máximo permitido no limiar de qualidade. Calculado sobre o valor mensal do serviço.

9.9.1. Para efeito de aplicação desta penalidade considera-se inexecução parcial o **IDM** com valor inferior a 90% e inexecução total o **IDM** com valor inferior a 85%.

9.9.1.1. Por inexecução parcial ou total do contrato, a CONTRATADA estará sujeita a glosa de 15% (quinze por cento) sobre a parte não executada, ou sobre o valor total do contrato;

9.9.1.2. A inexecução total ensejará a abertura de processo administrativo para apuração de responsabilidade e eventual penalização, sem prejuízo da aplicação da glosa prevista no item 9.9.1.1.

9.10. É vedada a subcontratação total dos serviços objeto deste Termo, sendo admitida a subcontratação parcial de até 20% do total contratado.

9.10.1. A subcontratação depende de autorização prévia da Contratante, a quem incumbe avaliar se a subcontratada cumpre os requisitos de qualificação técnica necessários para a execução do objeto;

9.10.2. Em qualquer hipótese de subcontratação, permanece a responsabilidade integral da Contratada pela perfeita execução contratual, cabendo-lhe realizar a supervisão e coordenação das atividades da subcontratada, bem como responder perante a Contratante pelo rigoroso cumprimento das obrigações contratuais correspondentes ao objeto da subcontratação;

9.10.3. Justifica-se a possibilidade de subcontratação para atendimento de atividades de maior complexidade técnica e atualização tecnológica que demandem a execução por um profissional especializado.

10. GARANTIA DA CONTRATAÇÃO

10.1. Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, no percentual de 5% do valor contratual, conforme regras previstas no contrato;

10.2. A garantia nas modalidades caução e fiança bancária deverá ser prestada em até 15 dias após a assinatura do contrato;

10.3. No caso de seguro-garantia, sua apresentação deverá ocorrer, no máximo, até a data de assinatura do

contrato;

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

11. MODELO DE EXECUÇÃO DO OBJETO

11.1. A execução do objeto consistirá no fornecimento de equipamentos e componentes, instalação e suporte técnico do fabricante, conforme especificações contidas no ANEXO I deste documento.

11.2. Após a assinatura da ata de registro de preços, a solicitação de execução do objeto será requerida pelo gestor da contratação mediante pedido de compra e, após emissão do empenho, formalizada por contrato.

11.2.1. O TRF6 irá requerer a execução de forma parcelada dos itens.

11.3. Assinado o contrato, o gestor convocará o responsável pela CONTRATADA para a reunião inicial e emitirá a Ordem de Fornecimento dos equipamentos nos prazos fixados no cronograma de execução, item 11.8.1 deste documento.

11.4. A contratada deverá entregar o Plano de Implantação dos produtos e serviços previstos nos Lotes 01 a 03, no prazo de 30 (trinta) dias corridos contados da emissão da Ordem de Fornecimento.

11.4.1. O Plano de Implantação deverá dispor sobre o cronograma de implantação da solução contratada, previsão de recursos, pessoas envolvidas, atividades a serem desenvolvidas pelo CONTRATANTE e pela CONTRATADA, além de indicar os principais riscos e forma de mitigação.

11.5. Aprovado o Plano de Implantação pelo CONTRATANTE, a contratada deverá executar o objeto em conformidade com as determinações dos fabricantes, normas técnicas pertinentes, especificações constantes na proposta apresentada e, ainda, de acordo com as Ordens de Serviços demandadas pelo CONTRATANTE.

11.6. Os bens e serviços deverão ser entregues no prazo máximo de 90 (noventa) dias corridos a contar da emissão da Ordem de Fornecimento, no horário das 9h às 18h, no seguinte endereço:

11.6.1. Subsecretaria de Infraestrutura - SUINF, situada na Av. Álvares Cabral, nº 1.805, 5º andar, Bairro Santo Agostinho, Belo Horizonte - MG, CEP 30.170-008. Contato pelo telefone: (31) 3501-1201;

11.6.2. Deverão ser entregues pela CONTRATADA todos os itens acessórios de hardware e software necessários à perfeita instalação e funcionamento, incluindo cabos, conectores, interfaces, suportes, em plena compatibilidade com a especificação técnica.

11.7. Após o recebimento definitivo dos equipamentos, será emitida a Ordem de Serviço da instalação dos equipamentos, que deverá ser realizada em conformidade com o Plano de Implantação e no prazo de até 30 (trinta) dias corridos da emissão da respectiva Ordem de Serviço;

11.8. Cronograma de Execução

11.8.1. O cronograma segue detalhado na tabela abaixo:

Ordem	Cronograma das Atividades	Prazo
1	Assinatura do contrato	Até 5 (cinco) dias úteis após regular convocação
2	Reunião inicial do contrato	Até 10 (dez) dias úteis da assinatura do contrato
3	Emissão da Ordem de Fornecimento dos equipamentos e respectivos licenciamentos (lote 01) e/ou licenciamentos (lotes 02 e 03)	Até 30 (trinta) dias corridos após a assinatura do contrato
4	Apresentação do Plano de Implantação (lotes 01 a 03)	Até 30 (trinta) dias corridos contados da emissão da Ordem de Fornecimento
5	Aprovação do Plano de Implantação (lotes 01 a 03)	Até 5 (cinco) dias corridos contados do recebimento do Plano de Implantação
6	Entrega dos equipamentos (lote 01) e/ou licenciamentos (lotes 02 e 03)	Até 90 (noventa) dias corridos contados da emissão da Ordem de Fornecimento
7	Emissão do Termo de Recebimento Provisório dos equipamentos e respectivos licenciamentos (lote 01) e/ou licenciamentos (lotes 02 e 03)	Até 5 (cinco) dias corridos contados da comunicação formal da entrega
8	Emissão do Termo de Recebimento Definitivo dos equipamentos e respectivos licenciamentos (lote 01) e/ou licenciamentos (lotes 02 e 03)	Até 10 (dez) dias corridos contados da emissão do Termo de Recebimento Provisório
9	Emissão da Ordem de Serviço de instalação	Após a emissão do Termo de Recebimento Definitivo
10	Instalação e configuração dos equipamentos	Até 30 (trinta) dias corridos contados da emissão da Ordem de Serviço de instalação
11	Emissão do Termo de Recebimento Provisório dos serviços de instalação	Até 5 (cinco) dias corridos contados da emissão da comunicação formal do fim da instalação pela CONTRATADA
12	Emissão do Termo de Recebimento Definitivo dos serviços de instalação	Até 10 (dez) dias corridos contados da emissão do Termo de Recebimento Provisório da instalação

12. MODELO DE GESTÃO DO CONTRATO

12.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial;

12.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila;

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

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

12.5. No momento de celebração do contrato será exigida declaração, firmada pelo representante legal da fornecedora licitante, de que possui em seu quadro de empregados pelo menos 02 (dois) profissionais com certificação técnica, tais como NSE4, CCNP Security, CCSE, PCNSE, F5-CSE Security, CompTIA Network+, CompTIA Cloud, Akamai GCSE/GCSA, Checkpoint CCSPA, Fortinet FCSS, ZTNA2.0 Palo Alto ou equivalente;

12.5.1. Devem ser apresentados junto à declaração:

12.5.1.1. Comprovante de vínculo trabalhista;

12.5.1.2. Cópia do Certificado.

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

12.7. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos;

12.8. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração;

12.8.1. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados;

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

12.8.3. O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso;

12.8.4. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato;

12.8.5. O fiscal técnico comunicará à Seção de Contratos, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou à prorrogação contratual;

12.8.6. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência.

12.9. O fiscal administrativo do contrato verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário;

12.9.1. Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando à autoridade competente para que tome as providências cabíveis, quando ultrapassar a sua competência.

12.10. O gestor do contrato coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração;

12.10.1. O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais;

12.10.2. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações;

12.10.3. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso.

12.11. O fiscal administrativo do contrato comunicará à Seção de Contratos - SETRA, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou prorrogação contratual;

12.12. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração;

12.1. O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do

contrato.

13. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

13.1. Do recebimento

13.1.1. Os serviços serão recebidos provisoriamente, no prazo previsto no item 11.8 - Cronograma de Execução, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo;

13.1.2. O prazo da disposição acima será contado do recebimento de comunicação oriunda do contratado com a comprovação da prestação dos serviços;

13.1.2.1. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico;

13.1.2.2. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo;

13.1.2.3. O fiscal setorial do contrato, quando houver, realizará o recebimento provisório sob o ponto de vista técnico e administrativo.

13.1.3. Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal técnico do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato;

13.1.3.1. O Contratado fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório;

13.1.3.2. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório;

13.1.3.3. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis;

13.1.3.4. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

13.1.4. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo;

13.1.5. Os serviços serão recebidos definitivamente no prazo no item 11.8 - Cronograma de Execução, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

13.1.5.1. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento;

13.1.5.2. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à CONTRATADA, por escrito, as respectivas correções;

13.1.5.3. Emitir Termo Circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas;

13.1.5.4. Comunicar a fornecedora para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização;

13.1.5.5. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.

13.1.6. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que concerne à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento;

13.1.7. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança;

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

13.2. Da liquidação

13.2.1. A liquidação do objeto seguirá o detalhamento do quadro abaixo:

LOTES	ITENS	CATMAT / CATSER	SERVIÇOS	UNIDADES REFERENCIAIS	LIQUIDAÇÃO
01	01	484747	Appliances de Next Generation Firewall	Unidade	Imediata
	02	27472	Licenciamentos para operações de Next Generation Firewall por 60 meses	Conjunto	Imediata
	03	26972	Instalação e Configuração	Conjunto	Imediata
	04	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	Mensalmente
	05	3840	Treinamento	Turma	Imediata
02	06	27472	Web Application Firewall - Appliance Virtual	Unidade	Imediata
	07	26972	Instalação e Configuração	Conjunto	Imediata
	08	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	Mensalmente
	09	3840	Treinamento	Turma	Imediata
03 a 10	10	27472	Serviço de Segurança de Borda (Security Service Edge - SSE)	Usuários	Por usuário e proporcionalmente à vigência contratual (*pro-rata*)
	11	26972	Instalação e Configuração	Conjunto	Imediata
	12	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	Mensalmente
	13	3840	Treinamento	Turma	Imediata

13.2.2. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022;

13.2.2.1. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, nos casos de contratações decorrentes de despesas cujos valores não ultrapassem o limite atualizado de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.

13.2.3. Para fins de liquidação, o setor competente deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

13.2.3.1. o prazo de validade;

13.2.3.2. a data da emissão;

13.2.3.3. os dados do contrato e do órgão contratante;

13.2.3.4. o período respectivo de execução do contrato;

13.2.3.5. o valor a pagar; e

13.2.3.6. eventual destaque do valor de retenções tributárias cabíveis.

13.2.4. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus à contratante;

13.2.5. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133/2021;

13.2.6. A Administração deverá realizar consulta ao SICAF para:

13.2.6.1. verificar a manutenção das condições de habilitação exigidas no edital;

13.2.6.2. identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.

13.2.7. Constatando-se, junto ao SICAF, a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do contratante;

13.2.8. Não havendo regularização ou sendo a defesa considerada improcedente, o contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos;

13.2.9. Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa;

13.2.10. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação junto ao SICAF.

13.3. Prazo de pagamento

13.3.1. O pagamento será efetuado no prazo máximo de até dez dias úteis, contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022;

13.3.2. No caso de atraso pelo Contratante, os valores devidos ao contratado serão atualizados

monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice IPCA de correção monetária.

13.4. Forma de pagamento

13.4.1. O pagamento será realizado através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado;

13.4.2. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento;

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

13.4.4. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente;

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

14. OBRIGAÇÕES DA CONTRATANTE

14.1. São obrigações do Contratante:

14.1.1. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o contrato e seus anexos;

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

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

14.1.4. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado;

14.1.5. Efetuar o pagamento ao Contratado do valor correspondente ao fornecimento do objeto, no prazo, forma e condições estabelecidos no presente Contrato;

14.1.6. Aplicar ao Contratado sanções motivadas pela inexecução total ou parcial do Contrato;

14.1.7. Cientificar o órgão de representação judicial da Advocacia-Geral da União, quando for o caso, para adoção das medidas cabíveis quando do descumprimento de obrigações pelo Contratado;

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

15. OBRIGAÇÕES DA CONTRATADA

15.1. O Contratado deve cumprir todas as obrigações constantes deste Termo de Referência, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:

15.1.1. Atender às determinações regulares emitidas pelo fiscal ou gestor do contrato ou autoridade superior;

15.1.2. Alocar os empregados necessários, com habilitação e conhecimento adequados, ao perfeito cumprimento das cláusulas deste contrato, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência;

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

15.1.4. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo Contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida no edital, o valor correspondente aos danos sofridos;

15.1.5. Não contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do contratante ou do Fiscal ou Gestor do contrato, nos termos do artigo 48, parágrafo único, da Lei nº 14.133, de 2021;

15.1.6. Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato, por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao Contratante;

15.1.7. Comunica ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços;

15.1.8. Prestar todo esclarecimento ou informação solicitada pelo Contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do empreendimento;

15.1.9. Paralisar, por determinação do Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas, bens de terceiros ou o patrimônio público;

15.1.10. Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à

execução do objeto, durante a vigência do contrato;

15.1.11. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos;

15.1.12. Submeter previamente, por escrito, ao Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congênere;

15.1.13. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;

15.1.14. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação;

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

15.1.16. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, II, d, da Lei nº 14.133, de 2021.

16. SANÇÕES ADMINISTRATIVAS

16.1. Os casos de inexecução não relacionados aos níveis de serviços, conforme previsões do item 9 deste termo de referência, serão tratados de acordo com o descrito a seguir.

16.1.1. Com fundamento nos artigos 155 e 156 da Lei nº 14.133/2021, a CONTRATADA ficará sujeita à aplicação das seguintes penalidades em caso de infrações administrativas:

a) advertência;

b) multa de:

b.1) 1% ao dia sobre o valor contratado, limitada a incidência a 10 (dez) dias, em razão do atraso injustificado na execução ou entrega dos serviços objeto do contrato, ou descumprimento dos prazos estabelecidos pela Administração para apresentação de documentos;

b.2) 15% sobre a parte não executada, em caso de inexecução parcial à qual tenha dado causa;

b.2.1) Para efeito de aplicação desta penalidade será considerado como inexecução parcial o não cumprimento dos níveis de serviços acordados, conforme disposições do item 9 deste termo de referência.

b.3) 15% sobre o valor contratado, em caso de inexecução total à qual tenha dado causa;

b.3.1) Para efeito de aplicação desta penalidade será considerada como inexecução total o não cumprimento dos níveis de serviços acordados, conforme disposições do item 9 deste termo de referência.

c) impedimento de licitar e contratar com a Justiça Federal de Primeiro Grau em Minas Gerais pelo prazo de até 03 (três) anos;

d) declaração de inidoneidade para licitar ou contratar com a Administração Pública pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos.

16.1.2. A penalidade de multa poderá ser aplicada cumulativamente às demais;

16.1.3. A aplicação da sanção de impedimento de licitar e contratar ou de declaração de inidoneidade para licitar ou contratar requererá a instauração de processo de responsabilização, ainda que decorrente de inexecução parcial do contrato;

16.1.4. A inexecução parcial ou total do contrato, por parte da CONTRATADA, poderá ensejar a resolução contratual, a critério da CONTRATANTE.

17. DA PROTEÇÃO DE DADOS

17.1. Na execução do objeto, devem ser observados os ditames da Lei 13.709/2018 (Lei Geral de Proteção de Dados) – LGPD, notadamente os relativos às medidas de segurança e controle para proteção dos dados pessoais a que tiver acesso mercê da relação jurídica estabelecida, mediante adoção de boas práticas e de mecanismos eficazes que evitem acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito de dados.

17.2. A contratada obriga-se a dar conhecimento formal a seus prepostos, empregados ou colaboradores das disposições relacionadas à proteção de dados e a informações sigilosas, na forma da Lei 13.709/2018 (LGPD), da Resolução/ CNJ 363/2021 e da Lei 12.527/2011.

17.2.1. Obriga-se também a comunicar à Administração, em até 24 (vinte e quatro) horas, contadas do instante do conhecimento, a ocorrência de acessos não autorizados a dados pessoais, de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou de qualquer outra forma de tratamento inadequado, suspeito ou ilícito, sem prejuízo das medidas previstas no art. 48 da Lei 13.709/2018 (LGPD).

17.3. O tratamento de dados pessoais dar-se-á de acordo com os princípios e as hipóteses previstas nos arts. 6º, 7º e 11 da Lei 13.709/2018 (LGPD), limitado ao estritamente necessário à consecução do objeto, na forma deste instrumento e seus anexos.

17.3.1. Para os fins de publicidade e transparência ativa sobre as contratações da Seccional, adota-se o entendimento do Parecer n. 00295/2020/CONJUR-CGU/CGU/AGU, segundo o qual tratamento de dados na

contratação de microempreendedor individual (MEI) contempla a divulgação de nome da pessoa física e do CPF, por serem dados que compõem, obrigatoriamente, a identificação empresarial.

17.4. É vedado, na execução do ajuste, revelar, copiar, transmitir, reproduzir, transportar ou utilizar dados pessoais ou informações sigilosas a que tiver acesso prepostos, empregados ou colaboradores direta ou indiretamente envolvidos na realização de serviços, produção ou fornecimento de bens. Para tanto, devem ser observados as medidas e os procedimentos de segurança das informações resultantes da aplicação da Lei 13.709/2018 (LGPD) e do parágrafo único do art. 26 da Lei 12.527/2011.

17.5. Em razão do vínculo mantido, na hipótese de dano patrimonial, moral, individual ou coletivo decorrente de violação à legislação de proteção de dados pessoais ou de indevido acesso a informações sigilosas ou transmissão destas por qualquer meio, a responsabilização dar-se-á na forma da Lei 13.709/2018 (LGPD) e da Lei 12.527/2011.

17.6. Extinto o ajuste ou alcançado o objeto que encerre tratamento de dados, estes serão eliminados, inclusive toda e qualquer cópia deles porventura existente, seja em formato físico ou digital, autorizada a conservação conforme as hipóteses previstas no art. 16 da Lei 13.709/2018 (LGPD).

17.7. A atuação da Seccional em relação aos dados pessoais dos contratados será regida pela Política de Proteção de Dados Pessoais – PPDP da Justiça Federal da 1ª Região, nos termos da Resolução PRESI 49/2021, notadamente pelos Art. 3º, 10, 11, 13 e 17, sem prejuízo da transparência ativa imposta pela legislação vigente:

> *"Art. 3º A PPDP se aplica a qualquer operação de tratamento de dados pessoais realizada pela Justiça Federal da 1ª Região, por meio do relacionamento com os usuários de serviços jurisdicionais e com os magistrados, servidores, colaboradores, fornecedores e terceiros, que fazem referência aos dados pessoais custodiados dessas relações.*
>
> *Art. 10. Em atendimento a suas competências legais, a Justiça Federal da 1ª Região poderá, no estrito limite das atividades jurisdicionais, tratar dados pessoais com dispensa de obtenção de consentimento pelos respectivos titulares. Parágrafo único. Eventuais atividades que transcendam o escopo da função jurisdicional estarão sujeitas à obtenção de consentimento dos interessados.*
>
> *Art. 11. A Justiça Federal da 1ª Região deve manter contratações com terceiros para o fornecimento de produtos ou a prestação de serviços necessários a suas operações. Esses contratos poderão, conforme o caso, sem prejuízo da transparência ativa imposta pela legislação vigente, importar em disciplina própria de proteção de dados pessoais, a qual deverá estar disponível a ser consultada pelos interessados.*
>
> *Art. 13. A responsabilidade da Justiça Federal da 1ª Região pelo tratamento de dados pessoais se sujeita aos normativos de proteção de dados vigentes, além do dever de empregar boas práticas de governança e segurança.*
>
> *Art. 17. O uso compartilhado de dados será realizado no cumprimento de suas obrigações legais ou regulatórias, com organizações públicas ou privadas, de acordo com a finalidade admitida na legislação pertinente, resguardados os princípios de proteção de dados pessoais."*

18. ADEQUAÇÃO ORÇAMENTÁRIA E ESTIMATIVA DE PREÇO

18.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União.

18.2. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

18.3. O custo total estimado para as aquisições e prestações dos serviços objetos deste Termo de Referência é de R$ 59.760.238,66, conforme quadro de preços abaixo:

LOTES	ITENS	CATMAT / CATSER	SERVIÇOS	UNIDADES REFERENCIAIS	QUANTIDADES	VALORES UNITÁRIOS ESTIMADOS 60 MESES (R$)	VALORES TOTAIS ESTIMADOS 60 MESES (R$)	VALORES TOTAIS ESTIMADOS (R$)
01	01	484747	Appliances de Next Generation Firewall	Unidade	2	974.227,92	1.948.455,84	5.338.404,73
	02	27472	Licenciamentos para operações de Next Generation Firewall por 60 meses	Conjunto	1	2.172.763,87	2.172.763,87	
	03	26972	Instalação e Configuração	Conjunto	1	113.861,27	113.861,27	
	04	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60	16.615,48	996.928,80	
	05	3840	Treinamento	Turma	1	106.394,95	106.394,95	
	06	27472	Web Application Firewall - Appliance Virtual	Unidade	1	1.179.426,29	1.179.426,29	

02	07	26972	Instalação e Configuração	Conjunto	1	110.014,51	110.014,51	1.719.254,43
	08	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60	6.786,30	407.178,00	
	09	3840	Treinamento	Turma	1	22.635,63	22.635,63	
03 - 10 *	10	27472	Serviço de Segurança de Borda (Security Service Edge - SSE)	Usuários	12.650	2.858,43	36.159.139,50	52.702.579,50
	11	26972	Instalação e Configuração	Conjunto	8	93.600,00	748.800,00	
	12	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	480	31.123,00	14.939.040,00	
	13	3840	Treinamento	Turma	8	106.950,00	855.600,00	

* Valores referentes ao órgão gerenciador e aos 7 (sete) órgãos participantes.

19. EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

19.1. A Equipe de Planejamento da Contratação foi instituída pela PORTARIA TRF6-SECOF 10/2024 (SEI Nº 0779055);

19.2. O presente termo de referência é assinado pela equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC, certificando que as diretrizes estabelecidas são as adequadas ao atendimento do interesse público envolvido e à caracterização da contratação, estando o documento compatível com o estudo técnico preliminar da contratação e apto à aprovação pela autoridade competente.

Integrante Requisitante	**Integrante Técnico**	**Integrante Administrativo**
Nome: Heli Lopes Rios Diretor da Subsecretaria de Infraestrutura - SUINF / SECTI Matrícula: TR 38	Nome: Arianne Caldeira do Carmo Diretora do Núcleo de Defesa Cibernética e Tratamento de Incidentes de Segurança da Informação - NUDCI Matrícula: TR 587	Nome: Fernanda Marília Gonçalves Caetano Assessor I - SULIC Matrícula: TR 578
O presente planejamento está em conformidade com os requisitos técnicos necessários ao cumprimento do objeto e atende adequadamente às demandas de negócio formuladas. Os benefícios pretendidos são adequados, os riscos envolvidos são administráveis, os custos previstos são compatíveis e caracterizam a economicidade.		

Autoridade Máxima da Área de TI
Nome: Daniel Santos Rodrigues Diretor da Secretaria de Tecnologia da Informação - SECTI/TRF6 Matrícula: TR 44
O presente planejamento está em conformidade com os requisitos técnicos necessários ao cumprimento do objeto e atende adequadamente às demandas de negócio formuladas. Os benefícios pretendidos são adequados, os riscos envolvidos são administráveis, os custos previstos são compatíveis e caracterizam a economicidade, **pelo que aprovo o artefato e encaminho para prosseguimento da contratação**.

Documento assinado eletronicamente por **Heli Lopes Rios**, **Diretor(a) de Subsecretaria**, em 11/02/2025, às 14:28, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Arianne Caldeira do Carmo**, **Diretor(a) de Núcleo**, em 11/02/2025, às 14:29, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Daniel Santos Rodrigues**, **Diretor(a) de Secretaria**, em 11/02/2025, às 14:45, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Fernanda Marília Gonçalves Caetano**, **Assessor(a) I**, em 11/02/2025, às 15:12, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

ANEXO

ANEXO I - ESPECIFICAÇÕES

1. LOTE 1. FIREWALL

1.1. Características Gerais

1.1.1. A solução deverá ser composta de hardware e software licenciado do mesmo fabricante;

1.1.2. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

1.1.3. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;

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

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

1.1.6. Os gateways de segurança, bem como a gerência centralizada, deverão suportar monitoramento através de SNMP v2 e v3;

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

1.1.8. Devem possuir homologação da Agência Nacional de Telecomunicações (ANATEL) conforme determina a Resolução nº 715, de 23 de outubro de 2019. Os documentos comprobatórios deverão ser apresentados na entrega dos equipamentos.

1.1.9. Para atendimento do Inciso III, Art. 3o do Decreto 7.174/2010, quando da entrega dos equipamentos, o licitante deverá comprovar a origem dos bens importados e apresentar comprovante de quitação dos tributos de importação a eles referentes, sob pena de suspensão do(s) pagamento(s), rescisão contratual e multa;

1.1.10. Não serão aceitas soluções em hardware de computadores pessoais (Personal Computers – PC) ou servidores, sendo obrigatório que o hardware e o software sejam do mesmo fabricante.

1.1.11. O fabricante deve ser parceiro do site www.cve.org, onde deverão estar indicados todos os CVE (Common Vulnerabilities and Exposures).

1.1.12. O fabricante deverá manter em seu site todos os CVE

identificados, seu detalhamento e correções disponibilizadas.

1.1.13. A solução deve estar posicionada entre os *challengers* e *leaders* no Quadrante Mágico do Gartner mais recente para solução de Network Firewalls;

1.1.13.1. O Gartner é um dos líderes mundiais em soluções de benchmarking de tecnologia e com o maior banco de dados do setor.

1.1.14. Deverá ser apresentado, ao menos um teste de laboratório (Nacional ou Internacional) que compare o seu produto com pelo menos outros 3 (três) fabricantes, garantindo-se que o equipamento ou outro da mesma série proposta possua efetividade de segurança acima de 70%;

1.1.14.1. Para o teste especificado acima, poderá ser utilizado como referência os testes realizados pela organização sem fins lucrativos CyberRatings.org, através de sua publicação "Enterprise firewall comparative security value map q2 2023";

1.1.15. Com o objetivo de estabelecer efetividade de segurança dos firewalls de nova geração e assegurar que o fornecedor tenha uma solução já testada e comprovada por um órgão independente de mercado, o equipamento proposto ou da mesma série proposta deverá:

1.1.15.1. Ser avaliado pela instituição NSS Labs (Network Security Services) no desempenho do Next Generation Firewall Comparative Analysis mais recente e deve constar no "Security Value Map" acima de 90% (noventa por cento); OU

1.1.15.2. Ser avaliado pela instituição NetSecOpen; OU

1.1.15.3. Ser avaliado pela instituição Miercom Certified Perfomance Verified; OU

1.1.15.4. Ser avaliado pela instituição Miercom Certified Secure.

1.2. Capacidades e Quantidades - Solução em Appliance de Segurança de Perímetro de Próxima Geração

1.2.1. Throughput de, no mínimo, 15 Gbps (Threat Protection/Prevention SEM SSL/TLS) e no mínimo 5.8 Gbps(Threat Protection/Prevention COM SSL/TLS), com as seguintes funcionalidades habilitadas:

1.2.1.1. Firewall;

1.2.1.2. Detecção e Prevenção de intrusão (IDS/IPS);

1.2.1.3. Controle de aplicação;

1.2.1.4. Filtro de URL;

1.2.1.5. Antivírus;

1.2.1.6. Anti-spyware;

1.2.1.7. Anti-phishing;

1.2.1.8. Bloqueio de arquivos e logs;

1.2.1.9. Prevenção de ameaças avançadas de dia zero;

1.2.1.10. Inspeção SSL/TLS;

1.2.2. O fabricante deve possuir documentação pública, descrevendo o perfil de tráfego;

1.2.3. A documentação deverá ser específica para o modelo ofertado, sob pena de desclassificação;

1.2.4. Suporte a, no mínimo, 5M (cinco milhões) de conexões simultâneas;

1.2.5. Suporte a, no mínimo, 250.000 (Duzentos e cinquenta mil) novas conexões por segundo;

1.2.6. Throughput de, no mínimo, 11 (onze) Gbps, no mínimo, para conexões VPN;

1.2.7. Suportar e estar licenciado para acesso remoto Client-to-site ilimitado ou com a licença de maior capacidade;

1.2.8. Fonte de alimentação redundante e hot-swappable;

1.2.9. O firewall deverá possuir memória suficiente para aguentar a performance exigida no edital durante todo o tempo do contrato;

1.2.10. No mínimo, 12 (doze) interfaces de rede 10Gbps SFP+;

1.2.11. No mínimo, 04 (quatro) interfaces de rede 10/100/1000;

1.2.12. No mínimo, 02 (duas) interfaces de 40G QSFP+;

1.2.13. Todas as interfaces devem vir acompanhadas do respectivo transceiver padrão Multimodo;

1.2.14. Possuir 1 (uma) interface de rede para sincronismo;

1.2.15. Possuir 1 (uma) interface de rede dedicada ao gerenciamento, não sendo permitido utilizar qualquer outra interface para exercer a função de gerenciamento do equipamento;

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

1.2.17. Cada um dos appliances da plataforma de proteção de rede deve possuir discos Solid State Drive (SSD) redundantes com no mínimo 480 GB de capacidade de armazenamento para o Sistema Operacional;

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

1.2.19. Suporte a RFC 4291 de Arquitetura de endereçamento IPv6;

1.2.20. Deve suportar Dual stack ipv4/ipv6 e NAT64;

1.2.21. Deve suportar NAT64 e NAT46;

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

1.2.23. Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP v4 e v6 sem duplicação da base de objetos e regras;

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

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

1.3. Funcionalidades de Firewall

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

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

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

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

1.3.5. Realizar upgrade via SCP ou SFTP e https via interface WEB;

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

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

1.3.6.2. Deverá suportar VXLAN;

1.3.7. Deve suportar os seguintes tipos de NAT:

1.3.7.1. Nat dinâmico (Many-to-1);

1.3.7.2. Nat estático (1-to-1);

1.3.7.3. Tradução de porta (PAT);

1.3.7.4. NAT de Origem;

1.3.7.5. NAT de Destino;

1.3.7.6. Suportar NAT de Origem e NAT de Destino simultaneamente;

1.3.8. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

1.3.9. As regras de NAT devem suportar “hit count” para monitorar a quantidade de conexões que deram matches em cada regra;

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

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

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

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

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

1.3.15. Suportar OSPF graceful restart;

1.3.16. Deve suportar roteamento ECMP (equal cost multi-path);

1.3.17. Para o ECMP, a solução deve suportar o balanceamento do roteamento de forma simultânea usando os seguintes parâmetros Origem, Destino, Porta de Origem, Porta de Destino e Protocolo;

1.3.18. Autenticação integrada via Kerberos;

1.3.19. A solução deve possuir mecanismo para dedicar processamento no equipamento de segurança para funções/ações de gerenciamento mesmo que o equipamento esteja com alto processamento de CPU, de forma a evitar a falta de acesso do administrador para qualquer mitigação de falha e aplicação de política para solução de problema.

1.3.20. As regras Firewall devem suportar “hit count” para monitorar a quantidade de conexões que deram matches em cada regra;

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

1.3.22. A solução deve permitir o agendamento de instalação de políticas para serem aplicadas em horários pré-definidos através da console centralizada **ou** permitir salvar as configurações das políticas para serem aplicadas em horários pré-definidos;

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

1.3.24. Deverá suportar redundância e balanceamento de links, tendo capacidade a no mínimo 3 links de internet;

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

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

1.4. Funcionalidades de Filtro de Conteúdo WEB

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

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

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

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

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

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

1.4.5.2. Reconhecer pelo menos 4.500 (quatro mil e quinhentas) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, *update* de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

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

1.4.7. Para inspeção SSL, ou HTTPS Inspection, a solução deve oferecer suporte ao HTTP/3 ou Perfect Forward Secrecy (conjuntos de cifras PFS, ECDHE);

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

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

1.4.10. A fim de otimização de tempo operacional dos administradores, a solução deverá possuir pelo menos 30 categorias ou subcategorias de aplicações WEB pré-definidas pelo fabricante;

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

1.4.12. Possuir mecanismo de controle de aplicação web e URL com configuração de bloqueio e liberação da aplicação principal e/ou as suas subcategorias. Quando o administrador da solução desejar bloquear apenas as sub-categorias do facebook, como facebook chat, vídeo, game, compartilhamento de arquivos ou outros. Ou seja, não deve ser bloqueado toda a categoria como “Facebook” ou “Redes sociais” que também pode implicar o bloqueio não só do Facebook, mas também bloqueará tudo que estiver relacionado às redes sociais, como LinkedIn, Twitter , YouTube, etc..

1.4.12.1. A solução precisa ser baseada em bloqueio de aplicações WEB que a própria base possui, assim a inspeção ocorrerá em camada 7 analisando o payload do pacote;

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

1.4.14. Atualizar a base de assinaturas de aplicações automaticamente;

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

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

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

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

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

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

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

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

1.4.23. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs atráves da integração com serviços de diretório, autenticação via Active Directory e base de dados local;

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

1.4.25. Suportar armazenamento, na própria solução ou na plataforma de gerencia local, de URLs, evitando delay de comunicação/validação das URLs;

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

1.4.27. Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja solução de software livre;

1.4.28. Suportar a criação de categorias de URLs customizadas;

1.4.29. Suportar a exclusão de URLs do bloqueio, por categoria;

1.4.30. Permitir a customização de página de bloqueio;

1.4.31. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede;

1.4.32. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius ou APIs ou Syslog, para a identificação de endereços IP e usuários;

1.4.33. Deve permitir o controle, sem instalação de cliente de software, em máquinas/computadores que solicitem saída à internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no Firewall (Captive Portal);

1.4.34. A solução deverá implementar uma análise avançada de URL em tempo real enviando a URL para o serviço de análise em cloud e não somente fazer a consulta em base local;

1.4.35. A filtragem de URL em tempo real deverá ser ativada por meio de filtragem de URL.

1.5. Funcionalidades de Prevenção de Ameaças

1.5.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus, Anti-Malware e Anti Phishing integrados no próprio equipamento de firewall;

1.5.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos;

1.5.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware e Anti-Phishing quando implementado em alta disponibilidade ativo/passivo;

1.5.4. Deve suportar granularidade nas políticas de Antivírus, Anti-Phishing e Anti-malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

1.5.5. A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo ou gerenciado automaticamente pelo SO;

1.5.6. Deverá possuir os seguintes mecanismos de inspeção de IPS:

1.5.6.1. Análise de padrões de estado de conexões, análise de decodificação de protocolo;

1.5.6.2. Análise para detecção de anomalias de protocolo;

1.5.6.3. IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

1.5.7. Detectar e bloquear a origem de portscans;

1.5.8. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

1.5.9. Possuir assinaturas para bloqueio de ataques de buffer overflow;

1.5.10. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;

1.5.11. Suportar bloqueio de arquivos por tipo;

1.5.12. Identificar e bloquear comunicação com botnets;

1.5.13. Deve suportar referência cruzada com CVE;

1.5.14. Em cada proteção de segurança, deve estar incluso informações como:

1.5.14.1. Código CVE (Common Vulnerabilities and Exposures), não sendo aceito outro código de referência;

1.5.14.2. Severidade;

1.5.14.3. Tipo de ação a ser executada;

1.5.15. O IPS deve fornecer um mecanismo automatizado para ativar ou gerenciar novas assinaturas vindas de atualizações.

1.5.16. O IPS deve suportar exceções de rede com base na origem, destino, serviço ou uma combinação dos três.

1.5.17. O IPS deve incluir um modo de solução de problemas que defina o perfil em uso para detectar apenas, sem modificar as proteções individuais.

1.5.18. O administrador deve poder ativar automaticamente novas proteções, com base em parâmetros configuráveis (impacto no desempenho, gravidade da ameaça, nível de confiança, proteção do cliente, proteção do servidor)

1.5.19. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

1.5.19.1. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;

1.5.20. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS através da console de gerência centralizada;

1.5.21. Na própria interface de gerência, a solução de IPS deverá apresentar sumário de todos os equipamentos que estão sendo gerenciados;

1.5.22. A solução de IPS, deve possuir mecanismo de análise baseado nas conexões realizadas para as aplicações, que aponta quais assinaturas que estão em modo detecção devem ser alterada para modo prevenção, assim evitando qualquer tipo de ataque para aplicações que estão expostas no ambiente.

1.5.23. O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados na funcionalidade de IPS;

1.5.24. A solução deverá possuir pelo menos dois perfis pré-configurados pelo fabricante que permitam sua utilização assim que o equipamento for configurado;

1.5.25. A solução deve permitir que o administrador possa configurar quais métodos e comandos HTTP são permitidos e quais são bloqueados.

1.5.26. Deve incluir proteção contra vírus em conteúdo ActiveX e applets Java e worms;

1.5.27. Solução deve proteger contra os ataques do tipo DNS Cache Poisoning, e impedir que os usuários acessem endereços de domínios bloqueados;

1.5.28. O gerenciamento centralizado via interface gráfica deve possibilitar a configuração de captura dos pacotes por regras individuais, visando aperfeiçoar o desempenho do equipamento;

1.5.29. A solução de IPS deve possuir engine com determinação de forma automática de qualquer nova assinatura que for baixada na base local;

1.5.29.1. Deverá atuar em modo de prevenção ou detecção, de forma a evitar qualquer tipo de alteração na base de assinatura

atual;

1.5.30. O antivírus deve oferecer suporte à verificação de links dentro de e-mails.

1.5.31. A solução de anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede quando usuário estiver conectado com ambiente externo malicioso.

1.5.32. A solução deve permitir criar regras de exceção de acordo com a proteção, a partir do log visualizado na interface gráfica da gerência centralizada;

1.5.33. Para melhor administração a solução deve possuir a granularidade na classificação das proteções de IPS através de: severidade, sistema operacional (minimamente Windows e Linux), target (cliente e servidor); ou nível de confiança da proteção, impacto da performance, referência de indústria terceira e status de download recente;;

1.5.34. A solução deve permitir a criação de White list baseado no MD5 do arquivo;

1.5.35. Os eventos devem identificar o país de onde partiu a ameaça;

1.5.36. Suportar rastreamento de vírus em arquivos pdf;

1.5.37. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);

1.5.38. Possuir a capacidade de prevenção de ameaças não conhecidas;

1.5.39. Em caso de falha no mecanismo de inspeção do Antivírus, deve ser possível configurar se as conexões serão permitidas ou bloqueada;

1.5.40. A solução de Antivírus e Antimalware deve funcionar de forma independente, ou seja, caso sejam desabilitadas, elas não podem causar a interrupção de outras funcionalidades de segurança como prevenção de ameaças avançadas (zero-day);

1.5.41. A solução Antivírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS/SMB, de forma a conter malwares se espalhando horizontalmente pela rede;

1.5.42. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;

1.5.43. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

1.5.44. Deverá possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos, sejam resolvidas pelo Firewall com endereços previamente definidos, para interceptar a comunicação e bloquear o acesso do usuário.

1.5.45. A solução de Antimalware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede.

1.5.46. A solução deve possuir funcionalidade de identificação de bloqueio de trafego malicioso comunicando com C&C (command & Control);

1.5.47. A solução Antivírus deverá suportar a análise de links no corpo de e-mails.

1.5.48. Modelos de deep learning em linha para prevenir tráfego C2 desconhecido e evasivo de ferramentas como Cobalt Strike e Empire;

1.5.49. Modelos de machine learning baseados na nuvem, atualizados regularmente, para prevenir explorações desconhecidas de injeção de comandos e injeção de SQL;

1.5.50. Bloqueio de ataques de malware na camada de rede com detecções baseadas em assinaturas em linha;

1.5.51. Assinaturas personalizadas para vulnerabilidades de software e ataques de command-and-control;

1.5.52. Análise baseada em heurísticas, decodificação de protocolos, proteção contra anomalias de protocolo e assinaturas de vulnerabilidades personalizadas;

1.5.53. Inspeção e classificação do tráfego, detectando e bloqueando malware e exploits de vulnerabilidades em uma única passagem;

1.5.54. Uso de AI, aprendizado de máquina e deep learning para detecção precisa de variantes avançadas de malware;

1.6. Funcionalidades de Controle de Qualidade de Serviço

1.6.1. Suportar a criação de políticas de QoS por: endereço de origem, endereço de destino e por porta;

1.6.2. O QoS deve possibilitar a definição de classes por: Banda garantida, banda máxima e fila de prioridade;

1.6.3. Disponibilizar estatísticas em tempo real para classes de QoS;

1.6.4. A solução deve permitir, por aplicação, o encaminhamento do tráfego para diferentes links de Internet, sejam eles locais ou remotos, deve suportar múltiplos links de acesso como MPLS, Internet Banda Larga, LTE (Private or Public APN) e Satélite;

1.6.5. Deve possibilitar a utilização de configuração inteligente de acessos WAN IP ativos-ativos sem a necessidade de switch para agregação WAN, ou seja, distribuir o tráfego simultaneamente pelos N acessos conectados e não apenas na configuração dos acessos principal e backup;

1.6.6. Medir parâmetros de rede jitter, perda de pacotes e latência em tempo real;

1.6.7. Se houver necessidade de saída internet do ponto remoto, deve ser possível selecionar por tipo de aplicativo;

1.6.8. Deve permitir a comunicação indireta entre localidades por meio de uma topologia “hub and spoke”;

1.6.9. Deve balancear o tráfego de aplicativos em vários links simultaneamente;

1.6.10. Redistribuição do tráfego balanceado, de forma inteligente, tendo em conta o congestionamento da largura de banda, entre os links utilizados, em caso de falhas nestes links, ou de acordo com as políticas de qualidade pré-definidas;

1.6.11. Habilitar a mesma interface WAN para enviar tráfego simultaneamente por meio de túneis IPSec SD-WAN e nativamente fora dos túneis via underlay;

1.6.12. Habilitar a criação de políticas de negócios para controlar o padrão de redirecionamento de tráfego e aplicar qualidade de serviço;

1.6.13. Suportar políticas inteligentes usando configuração padrão de fábrica que executem redirecionamento automático e imposição de QoS de voz, vídeo e tráfego transacional;

1.6.14. Suportar o redirecionamento do tráfego de internet de pontos remotos para um ponto de internet centralizado, usando políticas por aplicativo;

1.6.15. Redirecionamento condicionado do tráfego de internet em caso de falha do link de internet local ou do link remoto centralizado, utilizando políticas por aplicativo;

1.6.16. Suporte simultâneo ao redirecionamento do tráfego da Web de alguns aplicativos para a Internet centralizada, outros aplicativos para a Internet local e outros aplicativos para inspeção avançada de segurança na nuvem;

1.6.17. Implementar o conceito de perfis de configuração e grupos de objetos para automatizar o processo de implementação de políticas em grande escala;

1.6.18. Usar probes artificiais baseadas em icmp, udp ou tcp para medir a qualidade da rede percebida pelo tráfego do usuário, medindo no minimo jitter, latencia e perda de pacotes;

1.6.19. Capacidade de realizar agregação de largura de banda automaticamente entre links de diferentes velocidades, levando em consideração o uso total da largura de banda de cada link sem causar congestionamento em links de baixa velocidade;

1.6.20. Habilitar a configuração de backup do link, ou seja, um link de backup só deve ser ativado quando o link principal falhar;

1.6.21. Implementar um mecanismo de proteção de variação de latência (jitter) mesmo que a degradação esteja em todos os links, para proteger o tráfego em tempo real (voz e vídeo)de forma a priorizar este tráfego em conjunto com controle de qualidade do SD-Wan;

1.6.22. Garantir o desempenho de aplicativos em um cenário de link de transporte duplo quando ambo os links estão degradados simultaneamente;

1.6.23. Possuir um mecanismo de priorização (QoS) para proteger o tráfego de aplicativos clientes prioritários quando houver congestionamento em pontos remotos;

1.6.24. Deve automatizar o reconhecimento dos melhores níveis de SLA de rede com base no tipo de tráfego seja áudio, vídeo ou transacional;

1.6.25. O console de gerenciamento deve informar o status operacional (UP/DOWN/SPEED) das interfaces LAN e WAN;

1.6.26. O console de gerenciamento deve informar o status operacional de cada dispositivo que faz parte da rede para operacionalidade;

1.6.27. Realizar medições de “Latência”/”Jitter”/”Queda de pacotes” em cada um dos túneis SDWAN independentemente, na direção de

transmissão ou recepção;

1.6.28. O Orquestrador pode estar na Nuvem ou até mesmo ser instalado em um servidor dedicado ou virtualizado, utilizando uma máquina virtual;

1.6.29. No caso do Orchestrator estar na nuvem, a administração de atualizações, gerenciamento de alta disponibilidade e hardening do plano de gerenciamento deve ser realizada pelo fabricante da solução.

1.7. Funcionalidades de VPN

1.7.1. Suportar VPN Site-to-Site e Cliente-To-Site;

1.7.2. Suportar IPSec VPN;

1.7.3. A solução deve suportar Autoridade Certificadora Interna e Externa (de terceiros);

1.7.4. Suportar SSL VPN;

1.7.5. A VPN IPSEc deve suportar:

1.7.5.1. Algoritmos de criptografia 3DES, AES 128 e 256;

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

1.7.5.3. Algoritmo Internet Key Exchange (IKE) v1 e v2;

1.7.5.4. Autenticação via certificado IKE PKI;

1.7.5.5. Autenticação MD5, SHA-1, SHA-384,SHA-256, SHA-512;

1.7.6. A VPN SSL deve suportar:

1.7.6.1. Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

1.7.6.2. A funcionalidade de VPN SSL deve ser atendida com ou sem o uso de agente;

1.7.6.3. Suportar configuração de conformidade para acesso do usuário via portal SSL ou cliente na máquina do usuário;

1.7.6.4. Atribuição de endereço IP nos clientes remotos de VPN;

1.7.6.5. Atribuição de DNS nos clientes remotos de VPN;

1.7.6.6. Dever permitir criar políticas para tráfego dos clientes remotos conectados na VPN SSL.

1.7.7. A solução deve possuir checagem de conformidade e verificar, no mínimo, as seguintes informações no cliente remoto: sistema operacional e patches instalados, antivírus, firewall no host, chaves de registros e processos ativos;

1.7.8. A solução deve permitir bloquear o acesso do usuários aos recursos via VPN caso o usuário não esteja em conformidade com a verificação dos parâmetros configurados;

1.7.9. Suportar autenticação via AD/LDAP, certificado e base de usuários local;

1.7.10. A solução deve permitir a integração da ferramenta com provedores de identidade, atraves de SAML, para autenticação dos

usuários remotos conectados via VPN;

1.7.11. Suportar leitura e verificação de CRL (certificate revocation list);

1.7.12. A tecnologia de VPN Client to Server deverá ser instalada na plataforma: iOS 10 ou superior e Android;

1.7.13. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows 7, Windows 10/11 e MacOS X.

1.8. Solução para Proteção Contra Ameaças Avançadas - Zero Day

1.8.1. A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT;

1.8.2. A solução deverá ser composta por hardware e software específicos (appliance) com sistema operacional especializado em sua versão mais atualizada ou nuvem do proprio fabricante que possui o conceito de sandboxing para prevenção de ataques zero-day;

1.8.3. Não será aceito soluções que dependa da estrutura de hypervisor do contratante para a analise de ameaças de dia zero, como Vmware ESXi, Microsoft HyperV, entre outros;

1.8.4. Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS), FTP e E-mail (SMTP/TLS) durante análise completa do arquivo no ambiente sandbox, sem que o mesmo seja entregue parcialmente ao cliente.

1.8.5. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;

1.8.6. Implementar, identificar e bloquear malwares de dia zero em links de e-mail e URLs conhecidas;

1.8.7. Ameaças trafegadas em protocolo SMTP, de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;

1.8.8. A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows 7, Windows 10/11, MacOS, Android, Linux assim como Office;

1.8.9. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas antes de entregar este arquivo para o cliente;

1.8.10. O conteúdo enviado para a solução de Sandboxing deverá ser feito automaticamente, sem a necessidade da interação do usuário/administrador para que o processo de análise seja realizado;

1.8.11. Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, dias da semana ou dias do mês assim como o período de cada atualização;

1.8.12. Toda análise dos arquivos deverá ser realizada em ambiente controlado Sandboxing em nuvem ou on-premisse em equipamentos dedicados para este fim do mesmo fabricante da solução ofertada.. Não serão aceitas soluções em servidores genéricos ou software livre;

1.8.13. A funcionalidade de prevenção de ameaças avançadas deve

ser habilitada e funcionar de forma independente das outras funcionalidades de segurança;

1.8.14. Toda análise deverá ser realizada em nuvem do próprio fabricante ou equipamento on-premisse do mesmo fabricante da solução;

1.8.15. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF acima de 10 Mb;

1.8.16. Deve implementar análise em sandbox, detecção e bloqueio de malwares em arquivos executáveis, DLLs, ZIP e criptografados em SSL;

1.8.17. Deve implementar análise em sandbox, detecção e bloqueio de malwares em arquivos java (.jar e class);

1.8.18. A solução deve suportar inspeção para o protocolo SMBv3;

1.8.19. O relatório das emulações deve apresentar de maneira detalhada as atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado;

1.8.20. Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas;

1.8.21. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;

1.8.22. Capacidade de análise, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, seven-z, exe, dll, rtf, csv, scr, todos os tipos de arquivos do Microsoft Office, arquivos do Mac OS X, arquivos do Linux(ELF), arquivos do Android Package Kit (APK), arquivos do Adobe Flash, arquivos de script(BAT,JS,VBS,PS1,script do Shell e HTA), análise de links em mensagens de e-mail e arquivos criptografados (TLS/SSL);

1.8.23. Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real e o bloqueio deve ser imediato, não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;

1.8.24. Possibilitar remoção de conteúdo ativo dinâmicos como macros, URLs, Java scripts e outros dos arquivos baixados, permitindo o download do arquivo original caso ele não seja malicioso;

1.8.25. A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;

1.8.26. A solução deve possuir mecanismo para identificar sites conhecidos e desconhecidos como phishing, analisando em tempo real a URL acessada.

1.8.27. A solução deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas informações em sites classificados como phishing;

1.8.28. O Mecanismo de classificação de anti-phishing deve atuar sem

a necessidade de instalação de agente na máquina do usuário;

1.8.29. Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:

1.8.29.1. Número de arquivos emulados;

1.8.29.2. Número de arquivos com malware;

1.8.30. A solução de prevenção de ameaças avançada, deve possuir capacidade de apresentar em seus logs, visibilidade de acordo com o framework ATT&CK Mitre Matrix, pontuando características de táticas e técnicas de acordo com a ameaça detectada/bloqueada pela solução. Caso a solução não possua determinada capacidade, poderá ser integrada com outra solução de mercado, não sendo ela soluções abertas;

1.8.31. A solução deve prover informação, seja por meio de relatório ou log, sobre as seguintes situações:

1.8.31.1. Quantidade arquivos emulados e ações aplicadas OU o tamanho máximo do arquivo emulado seja excedido;

1.8.31.2. Classificar dos arquivos minimamente com os tipos (limpos, suspeitos e maliciosos) ou o tempo máximo de emulação seja excedido.

1.9. Módulo de Gerência

1.9.1. A solução de gerência deverá ser separada dos gateways de segurança, que irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas neste documento, exceto Sandbox que poderá ser gerenciado individualmente;

1.9.2. Deve ser compatível com VMware ESXi com espaço de armazenamento para LOGs de no mínimo, 200GB/LOG/DIA de ingestão;

1.9.3. Caso a solução possua licenças relacionadas a capacidade de log indexados e armazenamento, deve ser ofertado, no mínimo, 200GB/log/dia de ingestão;

1.9.4. Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução;

1.9.5. Deve fornecer consultas de logs, geração de relatório das funcionalidades de segurança que estão ativadas nos NGFWs e telas de apresentação onde consta todo os principais eventos das funcionalidades de controle de aplicação web, filtro URL, prevenção de ameaças (IPS, Antivírus, Anti-phishing, Anti-Malware e Sandboxing);

1.9.6. Deve possuir solução de gerenciamento e administração centralizado, possibilitando o gerenciamento de diversos equipamentos de proteção de rede do mesmo fabricante desde que não sejam software livre;

1.9.7. O módulo de gerência deve ser capaz de gerenciar e administrar todas as soluções descritas neste termo podendo estar em uma gerência a parte;

1.9.8. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;

1.9.9. Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento;

1.9.10. O gerenciamento da solução deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS);

1.9.11. Todos os logs da solução devem ser indexados e seu licenciamento deve ser o de maior capacidade.

1.9.12. O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores;

1.9.13. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

1.9.14. Suportar criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração;

1.9.15. Suportar backup das configurações e rollback de configuração para a última configuração salva;

1.9.16. Suportar validação de regras antes da aplicação;

1.9.17. Suportar validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

1.9.18. Deve permitir a visualização dos logs de uma regra específica em tempo real e na mesma tela de configuração da regra selecionada;

1.9.19. Deve possibilitar a integração com outras soluções de SIEM de mercado desde que não sejam software livre;

1.9.20. Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

1.9.21. Deve apresentar eventos em um único portal (dashboard) e geração de relatório de todas as funcionalidades de segurança que estão ativadas nos GW’s de segurança, sendo que deve possuir relatório e telas de apresentação onde consta todo os principais eventos das funcionalidades de controle de aplicação web, filtro URL, prevenção de ameaças (IPS, Antivírus, Anti-Malware, Anti-phishing e Sandboxing);

1.9.22. A solução deve permitir o login de múltiplos usuários administradores simultâneos com perfil de escrita, possibilitando agilidade e rapidez no gerenciamento pelo grupo de administradores da solução.

1.9.23. A solução deve permitir a integração da ferramenta com provedores de identidade para autenticação dos administradores da solução via SAML 2.0;

1.9.24. A solução deve permitir revisar e aprovar alterações de políticas de segurança feitas por outros administradores.

1.9.25. A solução deve permitir criar perfis de administradores para realizar revisão/alteração das políticas de segurança, com no mínimo, os perfis de aprovador e solicitante.

1.9.26. A solução deverá enviar a solicitação de aprovação de políticas de segurança por pelo menos uma das seguintes formas, Email,

Requisição WEB ou Scripts.

1.9.27. Permitir criação de relatórios customizados via interface gráfica, sem necessidade de conhecer linguagens de banco de dados podendo utilizar de datasets pré customizados pelo fabricante;

1.9.28. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware), e URLs que passaram pela solução;

1.9.29. Deve ser possível exportar os logs em CSV ou TXT;

1.9.30. O visualizador de log deve ter um recurso de pesquisa de texto livre;

1.9.31. Deve possibilitar a geração de relatórios de eventos no formato PDF ou HTML;

1.9.32. Possibilitar rotação do log;

1.9.33. Suportar geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

1.9.33.1. Resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda;

1.9.33.2. Principais aplicações por taxa de transferência de bytes,

1.9.33.3. Principais hosts por número de ameaças identificadas;

1.9.33.4. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus, Antiphishing e Anti-Malware), de redes vinculadas a este tráfego;

1.9.34. Deve permitir a criação de relatórios personalizados;

1.9.35. O gerenciamento centralizado deverá ser entregue como appliance virtual e dever ser compatível/homologado com/para VMWare ESX (vSphere 5.1, 5.5 ou 6);

1.9.36. A solução de gerenciamento deve possui a capacidade de gerenciar outros Firewalls de segurança do mesmo fabricante mesmo estão em ambientes virtualizados e nuvens públicas (AWS e Azure) e nuvens privadas (VMWare NSX ou Cisco ACI);

1.9.37. Possui capacidade de integração com soluções de terceiros via API e também suportar configurações através de RestAPI;

1.9.38. Deve consolidar logs e relatórios de todos os dispositivos administrados;

1.9.39. Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;

1.9.40. Deverá possuir mecanismo de Drill-Down para navegação e análise dos logs em tempo real;

1.9.41. Nas opções de Drill-Down, deve ser possível identificar o usuário que fez determinado acesso;

1.9.42. Permitir que os relatórios possam ser salvos, enviados e impressos;

1.9.43. Deve permitir a criação de filtros com base em qualquer

característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino, etc;

1.9.44. A solução deve prover, no mínimo, as seguintes funcionalidade para análise avançada dos incidentes:

1.9.45. Visualizar quantidade de tráfego utilizado de aplicações e navegação;

1.9.46. Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;

1.9.47. A solução de correlação deve possuir mecanismo para detectar login de administradores em horários irregulares;

1.9.48. A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

1.9.49. Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando para tanto gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos;

1.9.50. Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory via Radius;

1.9.51. Permitir criações de políticas de acesso de usuários autenticada no Active Directory, de forma que reconheça os usuários de forma transparente;

1.9.52. Geração de painel e relatórios contendo mapas geográficos gerados em tempo real para a visualização das principais ameaças através de origens e destinos do tráfego gerado na Instituição;

1.9.53. A plataforma de gerência centralizada e monitoração deve possibilitar a visualização dos logs de Firewall, navegação web, conteúdo de arquivos, prevenção de ameaças e Sandbox, todos a partir de um único local centralizado possibilitando a procura correlacionada de logs em uma única tela, como, por exemplo, pesquisar logs de Antivírus e navegação web simultaneamente na mesma query de pesquisa.

1.9.54. O relatório das emulações (sandboxing) deve conter de maneira detalhada as atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado;

1.9.55. Possuir mecanismo para que logs antigos sejam removidos automaticamente;

1.9.56. Possuir a capacidade de personalização de gráficos como barra, linha e tabela;

1.9.57. Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;

1.9.58. Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU;

1.9.59. A solução deve possuir painéis de eventos em tempo real com

possibilidade de configuração das atualizações e frequências;

1.10. Capacitação Técnica

1.10.1. O treinamento deverá ser completo para contemplar a instalação, customização, operação e administração da solução de firewall para 5 (cinco) funcionários da CONTRATANTE, na modalidade de Ensino a Distância (EAD), online e ao vivo;

1.10.2. O treinamento deverá ser ministrado para turma especifica para a CONTRATANTE;

1.10.3. Serão aceitos cursos oficiais do fabricante da solução;

1.10.4. Deverá possuir módulos teóricos e práticos;

1.10.5. Os instrutores devem ser certificados pelo fabricante da solução para o treinamento;

1.10.6. O conteúdo dos cursos deverá abranger, minimamente, os seguintes tópicos:

1.10.6.1. Configuração – acesso e navegação na solução; comando de configurações básicas e avançadas; estrutura/arquitetura do sistema operacional dos equipamentos; configuração via CLI, GUI, Client e web;

1.10.6.2. Operação – comandos de gerenciamento e monitoramento da saúde dos recursos dos equipamentos; aplicação de bloqueios manuais e automáticos e criação de filtros;

1.10.7. Ao final do treinamento deve ser emitido certificado de conclusão para cada participante/aluno constando a carga horária e a ementa.

1.11. Instalação e configuração

1.11.1. Os serviços de instalação e configuração deverão ser executados por técnico(s) certificado(s) pelo fabricante;

1.11.2. Os serviços de instalação compreendem as atividades de planejamento, instalação física, instalação lógica e finalização da solução no ambiente da CONTRATADA.

1.11.3. Os serviços de configuração consistem em ajustar todos os parâmetros necessários (físicos e lógicos) para o funcionamento da solução e a sua adequação para funcionamento no ambiente da CONTRATADA atendendo aos requisitos dessa especificação;

1.11.4. Caberá à CONTRATADA todo o processo de planejamento, a instalação, a configuração, a integração, os testes e a compatibilidade dos equipamentos, que deverão ser integrados à infraestrutura de Tecnologia de Informação existente no local de instalação dos equipamentos;

1.11.5. A instalação compreenderá a migração das configurações e regras existentes no ambiente atual do CONTRATANTE, suportado por um cluster de firewalls checkpoint , assim como as demais configurações de segurança e disponibilidade.

1.12. Operação Assistida

1.12.1. A operação assistida deverá ocorrer durante 45 dias corridos a

partir da instalação e configuração da solução na CONTRATANTE;

1.12.2. O serviço de operação assistida é composto por um conjunto de atividades que permitem o treinamento e a capacitação da equipe da CONTRATANTE responsável pelas atividades de operação, manutenção preventiva e corretiva, transferindo todo o conhecimento e experiência necessária para a operação da solução;

1.12.3. Durante os 45 dias corridos, será prestado todo o suporte necessário para a operacionalidade da solução, minimizando o risco da implantação da solução e proporcionando as condições ideais para transferência da tecnologia envolvida em regime de treinamento enquanto trabalha, até que a CONTRATANTE possa assumir as atividades com sua própria equipe;

1.12.4. Durante a operação assistida também será necessário realizar, pela CONTRADADA, possíveis customizações e ajustes finais que forem identificados durante o período de instalação, configuração e operação assistida;

1.12.5. Por padrão, a prestação da operação assistida ocorrerá presencialmente nas dependências da CONTRATANTE ou remotamente a ser definido pela CONTRATANTE;

1.12.6. A CONTRATADA deverá fornecer suporte técnico especializado em formato de Banco de horas para a solução ofertada;

1.12.7. A CONTRATADA deverá realizar a prestação de serviço remoto no modelo de banco de horas com um total de 300h, observando-se o consumo máximo de 16h/mês para ser utilizado durante a vigência do contrato e com pagamento somente se forem utilizadas.

1.13. Suporte, manutenção e atualização de versão

1.13.1. O suporte técnico compreende o diagnóstico e identificação de problemas, apoio técnico na utilização, correção de erros, defeitos (bugs) ou mau funcionamento sobre qualquer funcionalidade, recurso, componente ou módulo disponível de forma nativa na solução de firewall, ou decorrente de qualquer adaptação (customização) e ajuste (tuning) efetuada pela CONTRATANTE;

1.13.2. O atendimento a um chamado de suporte deverá ocorrer por qualquer uma das seguintes formas: contato telefônico, envio de mensagem eletrônica (e-mail), acesso ao sítio (website) da CONTRATADA ou do fabricante da solução de firewall, com controle de acesso por senha;

1.13.3. O atendimento telefônico sempre que aplicável e viável, por meio de ligação local em Belo Horizonte/MG ou ligação interurbana gratuita (0800);

1.13.4. A CONTRATANTE poderá efetuar um número ilimitado de chamados técnicos para a CONTRATADA, por qualquer uma das formas disponíveis, durante vigência do contrato vinculado a este edital;

1.13.5. Na abertura ou registro de um chamado técnico, por qualquer uma das formas disponíveis, a CONTRATADA deverá informar: data e hora de abertura do chamado, descrição do chamado, nível de severidade do chamado e identificação completa do solicitante;

1.13.6. A CONTRATADA deverá retornar, via e-mail, a confirmação da

abertura do chamado técnico, doravante denominado confirmação do chamado, contemplando as seguintes informações na sua abertura: código de identificação do chamado, identificação do responsável da CONTRATADA pela abertura do chamado;

1.13.7. O atendimento ao chamado técnico pela CONTRATADA deverá ocorrer pelo menos por uma das seguintes formas: chamada telefônica, envio de mensagem eletrônica (e-mail), recursos disponíveis no sítio (site) do fabricante da solução de firewall ou da CONTRATADA, presencial ou suporte por acesso remoto;

1.13.8. Caso acionado o suporte direto do fabricante, este deverá ter atendimento em português. Caso contrário, a CONTRATADA deverá ser responsável por intermediar os contatos entre o fabricante e a CONTRATANTE;

1.13.9. Um chamado técnico somente será considerado contingenciado ou concluído com o aceite da CONTRATANTE, na forma de um visto na ordem de serviço correspondente ou aceite por e-mail ou ainda, diretamente no sistema oferecido pela CONTRATADA, caso esta forma seja utilizada;

1.13.10. Após apresentar uma solução de contorno para o chamado técnico, a CONTRATADA deverá retornar, via e-mail, a confirmação da execução do serviço, contemplando as seguintes informações: código de identificação do chamado, data e hora de conclusão do atendimento, descrição dos serviços executados e/ou da solução apresentada;

1.13.11. Em caso de adoção de solução de contorno, sem prejuízo da solução definitiva cabível, a CONTRATADA deverá emitir laudos, na periodicidade exigida pela CONTRATANTE, informando sobre a evolução dos trabalhos para solucionar o problema de forma definitiva;

1.13.12. Após apresentar uma solução definitiva para o CHAMADO TÉCNICO, a CONTRATADA deverá retornar, via e-mail, a confirmação da execução do serviço, contemplando as seguintes informações: código de identificação do chamado, data e hora de conclusão do atendimento, descrição dos serviços executados e/ou da solução apresentada;

1.13.13. Deverá ser garantido à CONTRATANTE o pleno acesso ao sítio (site) dos fabricantes dos produtos que compõem a solução de firewall, com direito a consultas a quaisquer bases de conhecimentos e fóruns de discussão disponíveis para seus usuários;

1.13.14. Caberá exclusivamente à CONTRATANTE a decisão de implantar ou não quaisquer atualizações de software fornecidos pela CONTRATADA;

1.13.15. A CONTRATADA deverá disponibilizar mecanismos para a atualização de software pelo download direto através da própria aplicação, pelo envio das mídias ou através de download no seu sítio (site) ou do fabricante do software em questão;

1.13.16. O serviço de manutenção consiste na correção de qualquer problema ou falha apresentados em componentes físicos ou lógicos da solução;

1.13.17. A atualização de software é uma alteração da versão anterior com o objetivo de implementar melhorias. Essas melhorias podem ser de usabilidade, correção de falhas, desempenho, adição de novas funcionalidades, etc.;

1.13.18. O prazo de atualização de todo software fornecido deve ser igual ao período de garantia do produto. Durante a vigência do contrato, a CONTRATANTE terá direito a todas atualizações de versão e release dos softwares.

1.14. Garantia

1.14.1. O(s) equipamento(s) que compõe(m) a solução devem estar em linha de fabricação até a data de assinatura do contrato e a data de final de suporte (end-of-support) deve ser após término do contrato desta solução;

1.14.2. O serviço de Garantia contempla garantir o correto e pleno funcionamento de todos os itens adquiridos, seja hardware, software e os componentes necessários para o funcionamento da solução;

1.14.3. A CONTRATADA deverá garantir a substituição de qualquer módulo defeituoso, incluindo hardware, software ou componentes necessários para o funcionamento da solução durante o prazo contratado; bem como o próprio equipamento se for necessário;

1.14.4. Não haverá custos adicionais para a CONTRATANTE de substituição de quaisquer componentes durante o período de garantia;

1.14.5. Prazo de garantia deverá ser de 60 meses.

2. LOTE 2. WEB APPLICATION FIREWALL APPLIANCE VIRTUAL

2.1. Características Gerais

2.1.1. Não serão aceitos produtos ou serviços do tipo demo, trial e open-source. A solução deve ser proprietária;

2.1.2. A solução de WAF deverá ser fornecida em appliance virtual;

2.1.3. O appliance virtual deverá ser compatível com VMWARE e KVM, além de estar disponível no marketplace da AWS, GCP e Azure para contratação no modelo Bring Your Own License (BYOL);

2.1.3.1. Caso não seja possível a instalação em ambiente *on premises*, o licenciamento poderá sere realizado em nuvem privada do fabricante desde que sem custos adicionais ao contratante.

2.1.4. A solução deve ser capaz de visualizar, via console, as informações de saúde e desempenho de todo o ambiente que a compõem, incluído softwares e equipamentos;

2.1.5. Possuir suporte a SNMP v2c e v3;

2.1.6. Enviar mensagens por e-mail e traps SNMP;

2.1.7. Os componentes da solução poderão ser executados num mesmo appliance, ou poderão ser distribuídos em múltiplos appliances, de acordo com a característica de cada produto, respeitadas as características de funcionamento e performance

exigidas neste edital;

2.1.8. A solução deverá ter o pleno funcionamento independentemente de conexão (física ou lógica) com o fabricante, exceto para atualizações de versões e de segurança;

2.1.9. Suportar IPV6;

2.1.10. A solução deverá possuir a capacidade para suportar a adição de novos componentes (hardware e/ou software) escaláveis sem causar interrupções no funcionamento da solução;

2.1.11. Apresentar uma relação descritiva dos componentes fornecidos, incluindo seus códigos comerciais;

2.1.12. Não será aceito equipamento do tipo NGFW (Next Generation Firewall).

2.2. Características do Appliance

2.2.1. Deve ser capaz de executar todas as suas funções de aprendizado, análise e proteção de tráfego web considerando pelo menos uma taxa de transferência de 1 Gbps;

2.2.2. A solução deve ter vários mecanismos de implantação (deployment) com pelo menos uma ponte transparente na linha (Bridge L2), Proxy Reverso. Deve possuir a capacidade de monitorar e auditar todos os acessos de modo (passivo) a fim de monitorar o tráfego sem fazer alterações na rede;

2.2.3. A solução deve permitir a integração nos modos proxy reverso explícito e proxy reverso transparente (Bridge L2);

2.2.4. A solução deve ter um impacto de milissegundos na latência da rede;

2.2.5. O sistema deve permitir a integração e envio de alertas para terceiros ou ferramentas de correlação (SIEM). Será permitido que a integração seja realizada através da exportação de eventos utilizando SYSLOG ou através de RestAPI;

2.2.6. O equipamento deve suportar o protocolo de gerenciamento de rede SNMP a ser monitorado por ferramentas de terceiros;

2.2.7. Todos os componentes da solução de WAF com recursos para efetuar o balanceamento de carga entre aplicações devem ser do mesmo fabricante dos appliances, ou serem homologados pelo mesmo, ou compatíveis com outros fabricantes, podendo a CONTRATANTE realizar diligência junto ao mesmo para esta comprovação quando da recepção técnica da solução. As funcionalidades de WAF e balanceamento de carga entre aplicações web do TRF6 podem ser ofertadas no mesmo applicance ou em appliances distintos;

2.2.8. A solução de WAF com balanceamento de carga entre aplicações Web ofertada de maneira integrada deve ser composta de no mínimo um cluster com dois applicances;

2.2.9. Caso a solução de WAF seja ofertada separadamente da solução balanceamento de carga entre aplicações Web, tanto a solução de WAF quanto a solução de balanceamento deve ser composta de no mínimo um cluster com dois applicances ou servidores cada;

2.2.10. A solução de WAF e a solução de balanceamento entre aplicações web devem ser do mesmo fabricante;

2.2.11. A capacidade de processamento da solução deverá seguir as melhores práticas de cada fabricante, considerando todos os requisitos de capacidade definidos nesta especificação, tais como: trafego, conectividade, conexões, requisições nível 7, requisições SSL, transações e compressão;

2.2.12. Deve possuir CPU e memória suficientes para atender aos throughputs definidos no edital tanto para WAF quanto para o balanceador sem degradação de performance da solução quando ativada simultaneamente as duas funcionalidades;

2.2.13. Os equipamentos que serão responsáveis pela inspeção de tráfego web e pelo balanceamento de carga para soluções ofertadas em appliances distintos, deverão suportar, cada um de forma independente, o throughput de pelo menos 1 (um) Gbps tanto para a funcionalidade de firewall de aplicação Web como para a funcionalidade de balanceamento de carga entre aplicações;

2.2.14. As soluções de WAF com balanceamento ofertadas no mesmo appliance deverão suportar o throughput de pelo menos 1 (um) Gbps em cada appliance do cluster.

2.3. Balanceamento, Cache e Aceleração Web

2.3.1. Deve suportar no mínimo 1 Gbps (um Gigabits por segundo) de inspeção de tráfego na camada 7. Para alcançar esse throughput será aceito que o equipamento faça cache, em memória RAM ou SSD, do conteúdo estático, como por exemplo imagens, após a sua primeira inspeção. Todo conteúdo estático permitido em cache não será reinspecionado até a expiração do cache;

2.3.2. A solução fornecida deverá operar em cluster oferecendo alta disponibilidade com tolerância a falhas, independentemente da quantidade de elementos que compõe o cluster;

2.3.3. Na falha de um dos elementos do cluster, não poderá haver nenhuma degradação ou indisponibilidade das aplicações;

2.3.4. Deve suportar configuração de mTLS em um virtual server de aplicação do TRF6;

2.3.5. Deve suportar configuração de mTLS por url e path de aplicação do TRF6;

2.3.6. A solução deve ser capaz de trabalhar com recursos de alta disponibilidade, permitindo a ligação de dois ou mais equipamentos possibilitando configurar um único IP dos recursos protegidos nos dois ou mais equipamentos;

2.3.7. Deve ser fornecido todos os recursos possíveis de redundância sem nenhuma despesa com licenças adicionais;

2.3.8. A solução deve permitir a configuração das interfaces de alta disponibilidade do cluster (heartbeat), com opções para:

2.3.8.1. Compartilhar a rede de heartbeat com a rede de dados;

2.3.8.2. Utilizar uma rede exclusiva para o heartbeat.

2.3.9. A solução deverá ser capaz de trabalhar no modo Ativo/Standby,

com equipamento de mesmo fabricante;

2.3.10. A solução deverá ser capaz de trabalhar no modo Ativo/Ativo, mantendo o status das conexões;

2.3.11. Aceita-se como Ativo-Ativo a utilização de dois endereços Virtuais, onde cada endereço fica ativo em um elemento e em espera no outro;

2.3.12. A solução deve suportar múltiplas tabelas de rotas independentes;

2.3.13. O equipamento, quando habilitado para mais de uma função (Server Load Balancing (SLB), Aceleração Web, etc.), deverá permitir a definição da importância da função, determinando quantidade de processamento (CPU e memória) serão alocados para cada tipo de funcionalidade;

2.3.14. A solução deve possuir capacidade para gerenciar os recursos disponíveis de acordo com as funções habilitadas nos equipamentos SLB, GSLB, aceleração Web, etc.;

2.3.15. A solução deverá suportar e estar licenciado para todas as aplicações comuns de um Switch Layer 7 (sete):

2.3.15.1. Server Load-Balancing;

2.3.15.2. Firewall Load-Balancing;

2.3.15.3. Proxy Load-Balancing;

2.3.16. A solução deverá possuir recursos para balancear servidores do TRF6 com qualquer hardware, sistema operacional e tipo de aplicação;

2.3.17. Suportar Balanceamento apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;

2.3.18. A solução deve permitir o encapsulamento, em camada 3, do tráfego entre o balanceador e o servidor para tráfego IPv4 e IPv6, quando o balanceamento é realizado apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;

2.3.19. A solução deve ser capaz de abrir um número reduzido de conexões TCP com o servidor e inserir os HTTP requests gerado pelos clientes nestas conexões, reduzindo a necessidade de estabelecimento de conexões nos servidores e aumentando a performance do serviço;

2.3.20. A solução deve suportar e estar licenciado para os seguintes métodos de balanceamento para as aplicações do TRF6:

2.3.20.1. Round Robin;

2.3.20.2. Least Connections;

2.3.20.3. Weighted Percentage (por peso);

2.3.20.4. Servidor ou equipamento com resposta mais rápida baseado no tráfego real;

2.3.21. Weighted Percentage dinâmico (baseado no número de conexões);

2.3.22. Dinâmico, baseado em parâmetros de um determinado servidor ou equipamento, coletados via SNMP ou WMI;

2.3.23. A solução deve ser capaz de balancear as novas sessões, preservando as sessões existentes no mesmo servidor e implementando persistência de sessão dos seguintes tipos:

2.3.23.1. Por cookie – inserção de um novo cookie na sessão;

2.3.23.2. Por cookie – utilização do valor do cookie da aplicação, sem adição de cookie;

2.3.23.3. Por endereço IP destino;

2.3.23.4. Por Endereço IP origem;

2.3.23.5. Por sessão SSL;

2.3.23.6. Através da análise da URL acessada;

2.3.23.7. Através da análise de qualquer parâmetro no header HTTP;

2.3.23.8. Através da análise de qualquer informação da porção de dados (camada 7);

2.3.24. A solução deve utilizar Cache Array Routing Protocol (CARP) no algoritmo de HASH ou utilizando algum protocolo ou solução similar;

2.3.25. A solução deverá suportar os seguintes métodos de monitoramento dos servidores reais:

2.3.25.1. Layer 3 – ICMP;

2.3.25.2. Conexões TCP e UDP pela respectiva porta no servidor;

2.3.26. Devem existir monitores predefinidos para, no mínimo, os seguintes protocolos: ICMP, HTTP, HTTPS, FTP, SMB, RADIUS, NNTP, RPC, LDAP, IMAP, SMTP, POP3, SIP, SOAP, SNMP. Caso não exista um monitor pré-definido deve ser possível criar um monitor de forma manual;

2.3.27. A solução deverá possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico;

2.3.28. A solução deverá possuir recursos para limitar o número de sessões estabelecidas com cada servidor virtual;

2.3.29. A solução deverá possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores;

2.3.30. A solução deve possuir as seguintes funcionalidades de segurança ativas e licenciadas:

2.3.30.1. Network Address Translation (NAT);

2.3.30.2. Proteção contra Denial of Service (DoS);

2.3.30.3. Proteção contra Syn flood;

2.3.30.4. Implementar Listas de Controle de Acesso (ACL);

2.3.30.5. Permitir o controle da resposta ICMP por servidor virtual;

2.3.30.6. Realizar Limpeza de cabeçalho HTTP;

2.3.30.7. Análise em Camada 7 de Protocolos, com alertas para violações na camada de Protocolo HTTP.

2.3.31. Possuir recursos para executar compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;

2.3.32. Deve ser possível definir qual tipo de compressão será habilitada (gzip1 a gzip9, deflate);

2.3.33. Deve ser possível definir compressão especificamente para certos tipos de objetos;

2.3.34. A solução deve possuir recursos para fazer aceleração de SSL, onde os certificados digitais são instalados no equipamento e as requisições HTTP são enviadas aos servidores sem criptografia;

2.3.35. A solução deve ser capaz de ser configurada para recriptografar em SSL a requisição ao enviar para o servidor, permitindo as demais otimizações em ambiente 100% criptografado;

2.3.36. Suportar a utilização de memória RAM como cache de objetos HTTP, para responder às requisições dos usuários sem utilizar recursos dos servidores;

2.3.37. Possuir capacidade, no uso do recurso de cache, em definir quais tipos de objeto serão armazenados em cache e quais nunca devem ser cacheados;

2.3.38. Garantir que o recurso de cache possa ajustado em relação a quantidade de memória que será utilizada para armazenar objetos;

2.3.39. Possuir a capacidade para determinar qual o tamanho máximo do objeto a ser cacheado;

2.3.40. Possuir a capacidade para determinar qual o tamanho do menor objeto a ser cacheado;

2.3.41. Possuir a capacidade para determinar a URI (Uniform Resource Identifiers) que deve ser cacheada;

2.3.42. Possuir a capacidade para ler, alterar e ignorar o parâmetro cache-control no cabeçalho HTTP;

2.3.43. Possuir a capacidade para inserir e alterar o parâmetro age header no cabeçalho HTTP;

2.3.44. Suporte a otimização do protocolo TCP para ajustes a parâmetros das conexões clientes e servidor;

2.3.45. A solução deve suportar Internet Content Adaptation Protocol (ICAP);

2.3.46. Deve ser capaz de realizar DHCP relay;

2.3.47. A Solução deve ter a capacidade de permitir a criação de MIBs customizadas;

2.3.48. A Solução deve ter suporte a sFlow;

2.3.49. A solução deve ter suporte a, no mínimo, TLS 1.2, SHA 2 Cipher e SHA256 hash;

2.3.50. A solução deve ser capaz de colocar em fila as requisições TCP que excedam a capacidade de conexões do grupo de servidores ou de um servidor. O balanceador não deverá descartar as conexões que excedam o número de conexões do servidor ou do grupo de servidores;

2.3.51. Deve ser possível configurar o tamanho máximo da fila;

2.3.52. Deve ser possível configurar o tempo máximo de permanência na fila;

2.3.53. A solução deve realizar Controle de Banda Estático para grupos de aplicações e rede;

2.3.54. A solução deve realizar Controle de Banda Dinâmico para grupos de aplicações e rede;

2.3.55. A solução deve realizar Controle de Banda baseado em domínio de roteamento;

2.3.56. A solução deve possuir suporte ao espelhamento de conexões FTP, Telnet, HTTP, UDP, SSL;

2.3.57. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra-ataques;

2.3.58. Permitir a criação de políticas através de interface gráfica web para manipulação de tráfego através de lógica para pelo menos os seguintes operadores: GEOIP, http-basic-auth, http-cookie, http-header, httphost, http-method, http-referer, http-set-cookie, http-status, http-uri e http-version;

2.3.59. Deve ser possível tomar as seguintes ações através dessas políticas:

2.3.59.1. Bloqueio de tráfego;

2.3.59.2. Reescrita e manipulação de URL;

2.3.59.3. Registro de tráfego (log);

2.3.59.4. Adição de informação no cabeçalho HTTP;

2.3.59.5. Redirecionamento do tráfego para um membro específico;

2.3.59.6. Selecionar uma política específica para Aplicação Web.

2.3.59.7. Deverá possuir inteligência artificial para detecção além das assinaturas pré-definidas.

2.4. Características de Proteção de Aplicações Web

2.4.1. A solução pode executar automaticamente varreduras de rede que permitem a descoberta de novos servidores e serviços nos protocolos HTTP e HTTPS;

2.4.2. A solução deve proteger a infraestrutura web das aplicações de ataques contra a camada de aplicação (Camada 7);

2.4.3. A solução deve fornecer a possibilidade de bloquear transações WEB de maneira preventiva, antes que elas cheguem via rede ao servidor;

2.4.4. Deve ser capaz de correlacionar eventos ou violações de políticas;

2.4.5. A solução deve detectar, alertar e bloquear opcionalmente, em tempo real, qualquer comportamento malicioso conhecido e/ou desconhecido;

2.4.6. A solução deve ter um modo de aprendizado que permita definir quais ações são esperadas e aceitas pelos usuários;

2.4.7. No modo de aprendizado, o sistema deve aprender a estrutura e os elementos do aplicativo e essas informações devem estar

disponíveis para automatizar a configuração do modelo de segurança positivo. Pelo menos você deve aprender sobre: Hosts válidos, URLs, parâmetros, cookies, tipo de conteúdo dos parâmetros;

2.4.8. No modo de aprendizado, deve aprender além do comportamento esperado do usuário e essas informações devem estar disponíveis para automatizar a configuração do modelo de segurança positivo. No mínimo, você deve aprender sobre: Caracteres aceitos, tamanho do valor esperado;

2.4.9. O modo de aprendizagem pode ser ativado e desativado manualmente para estender o tempo de reconhecimento do padrão de comportamento;

2.4.10. O modo de aprendizagem deve poder permanecer ativo mesmo quando está em modo de proteção ou bloqueio, permitindo a incorporação de novos parâmetros ou características do mesmo sem ter que fazê-lo manualmente. De tal forma que a configuração de segurança positiva é atualizada automaticamente e constantemente;

2.4.11. Com relação a quaisquer ataques ou outra atividade não autorizada, a solução deve ser capaz de tomar as medidas adequadas, pelo menos: Terminar solicitações e respostas, bloquear a sessão TCP, isolados em quarentena temporária ou bloquear o usuário do aplicativo, colocar em quarentena temporária ou bloquear o endereço IP de origem;

2.4.12. A solução deve ter um conjunto de padrões correspondentes aos ataques conhecidos. Esta base de dados de padrões deve poder ser atualizada periodicamente, automaticamente e sem ajuda;

2.4.13. A solução deve permitir a definição para as regras e alarmes, condições lógicas em que o alarme ou o bloqueio não sejam ativos se não aconteceu o evento, pelo menos, um número de vezes definido dentro de um período de tempo definido e associado a um contexto de conexão definível;

2.4.14. A solução deve ter a capacidade de proteger os serviços Web com base no SOAP;

2.4.15. A solução deve ter a capacidade de receber e usar certificados e pares de chaves pública / privada para servidores da Web protegidos;

2.4.16. A solução deve poder inspecionar e monitorar todos os dados HTTP/S do aplicativo, incluindo cabeçalhos HTTP, campos de formulário e o corpo de solicitações HTTP/S;

2.4.17. A solução deve inspecionar as solicitações e as respostas HTTP/S;

2.4.18. A solução deve ser capaz de validar todos os tipos de dados inseridos, incluindo URLs, formulários, cookies, consultas, campos e parâmetros ocultos, métodos HTTP, elementos XML e ações SOAP;

2.4.19. A solução deve ser capaz de identificar o usuário do aplicativo da Web. A identificação deve persistir até que o usuário tenha deixado o aplicativo;

2.4.20. A solução deve ser capaz de identificar e manter um registro das sessões da Web no nível do aplicativo, por meio de cookies de rastreamento ou parâmetros do aplicativo;

2.4.21. A solução deve ser capaz de aplicar uma correção virtual (virtual patching) para proteger as vulnerabilidades detectadas e deve ter integração com scanners de vulnerabilidade (pelo menos 3 soluções ou serviços diferentes do mercado) para receber os seus resultados ou relatórios, interpretar e sugerir mudanças para aplicar como correção virtual;

2.4.22. A solução deve suportar a detecção de ferramentas de download automático, bots, scripts, etc. através da geração de um requisito em JavaScript, a fim de bloquear todas as consultas que não possuem um navegador real por trás;

2.4.23. A solução deve ser capaz de implementar controles anti-scrapping de forma nativa, permitindo bloquear tentativas automatizadas de roubar informações do site;

2.4.24. A solução deve ser capaz de reconhecer IPs de fontes mal-intencionadas (como redes TOR, proxies anônimos, sites de Phishing, etc.) e também ter catalogação de IPs por geolocalização. Essas informações devem ser atualizadas periodicamente e deve ser possível integrar políticas de segurança como um critério;

2.4.25. Ser capaz de diferenciar entre as requisições legítimas realizadas por usuários humanos das requisições realizadas por bots, web scraping e ataques automatizados;

2.4.26. A solução deve fornecer proteção automatizada para todas as vulnerabilidades expressas no OWASP Top 10;

2.4.27. A solução deve permitir a geração de exceções para as políticas de segurança de validação de protocolo por URL ou IP de origem;

2.4.28. A solução deve permitir a inspeção das conexões SSL (SSL v3, TLS v1) implementadas nos servidores da web. Para isso, os certificados (chave pública e privada) podem ser importados;

2.4.29. A solução deve validar se o conteúdo e a duração do protocolo HTTP, incluindo os cabeçalhos, corpo e cookies, estão corretos. Por sua vez, você deve ser capaz de restringir os métodos HTTP usados em um aplicativo da Web (GET, POST, PUT, etc.);

2.4.30. A solução deve permitir ações e alertar para violações de protocolos inferiores ao aplicativo, incluindo inspeção de pacotes IP, TCP, UDP e seus cabeçalhos;

2.4.31. A solução deve proteger os aplicativos da Web contra ataques comuns, como:

2.4.31.1. Injeção SQL (SQL Injection);

2.4.31.2. Injeção de LDAP (LDAP Injection);

2.4.31.3. Comando do SO (SO Commanding);

2.4.31.4. Injeção SSI (SSI Injection);

2.4.31.5. Inclusão remota de arquivos (Remote File Inclusion);

2.4.31.6. Mail Command Injection;

2.4.31.7. Injeção de XML (XML Injection);

2.4.31.8. Injeção Xpath (XPath Injection);

2.4.31.9. Injeção Xquery (XQuery Injection);

2.4.31.10. Cross Site Scripting (XSS);

2.4.31.11. Cross Web Request Forgery (CSRF);

2.4.31.12. Web Scrapping;

2.4.31.13. Navegação forçada (Forceful Browsing).

2.4.32. Proteção de modificação de campos ocultos;

2.4.33. Permite a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;

2.4.34. A solução deve suportar a definição de políticas diferentes que podem ser associadas a cada aplicativo individualmente;

2.4.35. Para cada aplicação protegida, o administrador deve ser capaz de configurar em que momento é feita a detecção (log) dos ataques recebidos e quando eles evitam (bloqueiam) os ataques;

2.4.36. Para cada aplicativo da Web, deve ser possível desabilitar a prevenção de ataques (bloqueio) e deixar apenas a detecção (log) em formato granular para facilitar a solução de problemas por tipos de ataques;

2.4.37. No caso de um bloqueio, dependendo do modo de operação, a resposta (página) enviada ao usuário deve poder ser personalizada;

2.4.38. A solução deve permitir que hosts ou clientes confiáveis sejam excluídos das medidas de proteção;

2.4.39. A solução deve suportar a identificação do IP de origem no caso de passar por proxy, interpretando o campo X-forwarded-for do cabeçalho HTTP;

2.4.40. A solução deve validar se o conteúdo e a duração do protocolo HTTP, incluindo os cabeçalhos, corpo e cookies, estão corretos;

2.4.41. Deve possuir hardware dedicado para inspeção otimizada de tráfego criptografado com SSL e TLS;

2.4.42. A latência inserida no tráfego SSL não pode superar os 5ms (cinco milissegundos);

2.4.43. A solução deve suportar o uso de firewall camada 3 e 4 junto com firewall camada 7 no mesmo appliance para evitar problemas com o aumento da latência;

2.4.44. A solução deve suportar responder por 1 endereço IP e vários endereços IPs por aplicação web;

2.4.45. Deve poder atuar como Web Application Firewall em modo WAF Positivo (permitindo apenas o que é conhecido e esperado);

2.4.46. Deve poder atuar como Web Application Firewall em modo WAF Negativo (bloqueando características conhecidas de ataque);

2.4.47. Deve ser capaz de operar usando modelo positivo de segurança, por meio de aprendizado e de definição de regras que descrevem o comportamento esperado de um aplicativo ou serviço, efetuando o bloqueio de todo o tráfego que não coincide com essas regras (árvore de acesso válido);

2.4.48. Possuir as seguintes características:

2.4.48.1. Facilidade para liberação de regras aprendidas automaticamente que estejam gerando grande quantidade de falso positivo;

2.4.48.2. Facilidade para transformar um ataque detectado e considerado falso positivo como regra do firewall;

2.4.48.3. Facilidade para aplicar diferentes regras para diversas aplicações;

2.4.48.4. Capacidade para customizar regras de negação de serviço;

2.4.48.5. Capacidade para combinar detecção e prevenção na construção das regras;

2.4.48.6. Capacidade para desfazer a aplicação de uma regra.

2.4.49. Deve suportar o modelo de segurança positivo, devendo ser capaz de aprender qual perfil de tráfego é legítimo e bloquear ataques ou atividades não autorizadas;

2.4.50. Deve possuir políticas de segurança de aplicações web pré-configuradas na solução;

2.4.51. Deve permitir a criação de políticas diferenciadas por aplicação;

2.4.52. Deve possuir funcionalidade que ajuste dinamicamente o nível de proteção na detecção de ataques;

2.4.53. Deve ser possível utilizar uma política em múltiplas aplicações (uma para várias);

2.4.54. Deve ser possível utilizar uma política para cada aplicação (uma para uma);

2.4.55. Deverá possuir funcionalidade de criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real observado à aplicação;

2.4.56. O perfil aplicação aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;

2.4.57. Deve identificar e criar um perfil de utilização das aplicações, mesmo que as páginas Web e conteúdos sejam dinâmicos, como os desenvolvidos em JavaScript, CGI, ASP, PHP e Java;

2.4.58. Deve suportar WebSocket Traffic Filter;

2.4.59. Deve suportar o controle de política granular baseada no caminho do aplicativo (application path);

2.4.60. Deve permitir a aceitação de falsos positivos (exceção à política de segurança);

2.4.61. Deve permitir que ao detectar um falso positivo, o administrador aceite a requisição e atualize a política automaticamente;

2.4.62. Deve suportar a configuração de hosts confiáveis para permitir a execução de operações não permitidas pela política adotada para uso em eventos de testes de penetração, solução de problemas (troubleshooting) e análise de performance;

2.4.63. Deverá possuir proteção baseada em assinaturas para prover proteção contra-ataques conhecidos;

2.4.64. Deverá ser possível desabilitar algumas assinaturas específicas em determinados parâmetros, como uma exceção à regra geral;

2.4.65. As atualizações de assinaturas deverão passar por um período configurável de testes, onde nenhuma requisição que viole a assinatura será bloqueada, apenas informada no relatório. Este processo deve ser automatizado, não sendo necessário criar regras específicas a cada atualização de assinatura;

2.4.66. A solução deverá realizar bloqueios de ataques mesmo sem assinaturas atualizadas;

2.4.67. Deverá implementar consultas a bases de reputação externas;

2.4.68. A solução deve ser capaz de decifrar tráfego SSL a partir da importação de chaves criptográficas, para permitir a inspeção de todo conteúdo do pacote originalmente cifrado;

2.4.69. Inspeção de tráfego através da troca de chaves assimétricas entre cliente e WAF (proxy SSL);

2.4.70. A solução deve suportar SSL Offload de conexões;

2.4.71. A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação. Essa inspeção poderá ser feita via integração ICAP;

2.4.72. A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação;

2.4.73. Permitir a integração com Firewall de Database de outros fabricantes;

2.4.74. Deve possuir tecnologia de detecção de anomalias baseado nos IDs dos dispositivos, permitindo a detecção de DoS, ataques de força bruta e ataques de sequestro de sessão. Deve ser possível filtrar relatórios por IDs de dispositivos;

2.4.75. A solução deverá permitir proteção contra envio de arquivos, considerando tamanho e tipo;

2.4.76. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar e aumentar a proteção contra-ataques recentes;

2.4.77. A solução deve se integrar com outras soluções de segurança como firewall, IPS e análise de logs de outros fabricantes;

2.4.78. Deverá armazenar os logs localmente ou exportar para Syslog server;

2.4.79. Possuir registro de logs com as seguintes características:

2.4.79.1. Em cada registro de log de acesso deve ser inserido um identificador de transação HTTP que deve ser único, envolvendo o par requisição/resposta;

2.4.79.2. Os registros de log de acesso e eventos devem ser armazenados em arquivo ou em banco de dados que permita a exportação ou em outro formato aberto como CSV ou TXT, podendo ainda serem armazenados localmente ou carregados (upload) em servidor de log via FTP ou SCP ou armazenados em

servidor externo de banco de dados;

2.4.79.3. Permitir configurar a retenção dos logs por tempo e volume;

2.4.79.4. Ter capacidade para detecção, remoção ou codificação de dados sensíveis do log.

2.4.80. Deverá ser capaz de diferenciar acessos entre bots, Web scraping e usuários humanos para bloquear ataques automatizados;

2.4.81. Deve oferecer um serviço baseado na reputação do endereço IP de origem, protegendo as aplicações de serem acessadas pelas seguintes origens: Rede TOR, proxies anônimos e endereços IP de baixa reputação;

2.4.82. A Solução de Firewall de Aplicação deve suportar diferentes métodos de autenticação dos usuários das aplicações como: HTML Form, HTTP Basic Authentication, JSON/AJAX Request, NTLM, certificados SSL Client e HTTP Digest Authentication;

2.4.83. A solução deverá ser capaz de identificar e bloquear ataques através de:

2.4.83.1. Assinaturas, com atualização periódica da base pelo fabricante;

2.4.83.2. Regras de verificação personalizadas – política de segurança configurada;

2.4.83.3. Comportamento malicioso.

2.4.84. Deverá trabalhar com filtros de segurança:

2.4.84.1. De controle dos parâmetros das aplicações;

2.4.84.2. De proteção a sessão;

2.4.84.3. De controle de vulnerabilidades;

2.4.84.4. De controle de serviços Web;

6.2.4.84.5. De proteção a XML.

2.4.85. Permitir o bloqueio de ataques DoS/DDoS na camada 7, possuindo também a opção de apenas registrar o ataque, sem tomar nenhuma ação de bloqueio;

2.4.86. Não deve haver a necessidade de intervenção de usuário para configurar thresholds DoS pois esses valores devem ser autoajustáveis e adaptáveis de acordo com mudanças;

2.4.87. Possuir as seguintes formas de detecção de ataques DoS/DDoS na camada de aplicação:

2.4.87.1. Número de requisições por segundo enviados a uma URL específica;

2.4.87.2. Número de requisições por segundo enviados de um IP específico;

2.4.87.3. Detecção através de código executado no cliente com o objetivo de detectar interação humana ou comportamento de robôs (bots);

2.4.87.4. Número máximo de transações por segundo (TPS) de um determinado IP;

2.4.87.5. Aumento de um determinado percentual do número de transações por segundo (TPS);

2.4.87.6. Aumento do tempo de resposta (latência de aplicação) de uma determinada URL.

2.4.88. Deve permitir criar lista de exceção (whitelist) por endereço IP específico ou faixa de sub-rede;

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

2.4.90. Deverá permitir limitar o número de conexões e requisições por IP de origem para cada endereço IP Virtual;

2.4.91. Deve permitir adicionar, automaticamente e manualmente, em uma lista de bloqueio, os endereços IP de origem que ultrapassarem o limite estabelecido, por um período de tempo determinado através de configuração;

2.4.92. Permitir o bloqueio de determinados endereços IPs que ultrapassarem um número máximo de violações por minuto. O período de bloqueio deverá ser configurável e durante este período todas as requisições do cliente serão bloqueadas automaticamente;

2.4.93. A solução deve permitir o cadastro de robôs que podem acessar a aplicação;

2.4.94. Deve permitir o bloqueio de robôs (bots) que acessam a aplicação através de detecção automática, não dependendo de cadastros manuais;

2.4.95. Deve possuir mecanismo capaz de diferenciar entre bots e usuários humanos para bloquear ataques automatizados (robôs):

2.4.95.1. O mecanismo deve implementar mecanismos de desafios de Cookies, JavaScript e Captcha para reforçar a identificação de robôs;

2.4.95.2. O mecanismo deve consultar base de dados de robôs já conhecidos; 4.108.3 O mecanismo deve permitir a integração com o sistema de Captcha do Google.

2.4.96. Deverá permitir adoção de critérios de decisão para bloqueio e alerta, considerando no mínimo 7 (sete) critérios simultâneos, dentre eles:

2.4.96.1. Tempo de resposta de uma página web;

2.4.96.2. Tamanho da resposta de uma página web;

2.4.96.3. User-agent (navegador);

2.4.96.4. Usuário;

2.4.96.5. IP de origem

2.4.96.6. País de origem

2.4.96.7. Assinatura de ataque;

2.4.96.8. Conteúdo do payload;

2.4.96.9. Conteúdo do cabeçalho;

2.4.96.10. Conteúdo do cookie;

2.4.96.11. Código de resposta do servidor web;

2.4.96.12. Nome do host (Host Header);

2.4.96.13. Número de ocorrências num intervalo de tempo;

2.4.96.14. Método HTTP;

2.4.96.15. Horário.

2.4.97. Ao detectar um ataque ou qualquer atividade não autorizada, deve ser possível bloquear:

2.4.97.1. Requisições e respostas;

2.4.97.2. Uma conexão TCP;

2.4.97.3. Uma rede específica;

2.4.97.4. Um endereço IP durante um intervalo de tempo específico.

2.4.98. A solução deve fornecer, para cada política de segurança, múltiplas opções de evento posteriores ao bloqueio da requisição, dentre eles: Enviar log para Syslog Externo, enviar um e-mail, alerta para a interface de monitoração da gerência, executar um script definido pelo administrador e apresentar uma página de erro para o usuário;

2.4.99. Quando uma requisição for bloqueada pelo WAF, deve ser possível comunicar ao usuário sobre o fato através de uma página HTML informativa. 4.113 Deverá permitir a customização da resposta de bloqueio. Deve ser possível customizar a página HTML baseada em contextos como (Tipo de ataque, IP de Origem, Usuário e GeoLocalização) sendo configuradas através da GUI sem a necessidade de criação de scripts atém do HTML;

2.4.100. Deverá implementar proteção ao JSON (JavaScript Object Notation), REST (Representational State Transfer) e SOAP (Simple Object Access Protocol);

2.4.101. Deverá implementar proteção a API;

2.4.102. Deverá implementar proteção WebSockets;

2.4.103. Deverá implementar proteção sobre microsservicos;

2.4.104. Deve possuir suporte a filtro e validação de funções XML específicas da aplicação;

2.4.105. Prevenir o vazamento de informações, permitindo o bloqueio ou a remoção dos dados confidenciais;

2.4.106. Deve prevenir que erros de aplicação ou infraestrutura sejam mostrados ao usuário;

2.4.107. A solução deverá permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle;

2.4.108. A solução deverá ser capaz de interpretar o campo X-Forwarded-For como endereço IP de origem original de um pacote, a fim de identificar a origem real de tráfego que sofra NAT de origem;

2.4.109. Deverá proteger contra-ataques CSRF (Cross-Site Request Forgery), podendo ser possível especificar quais URLs serão examinadas;

2.4.110. A Solução deverá proteger, no mínimo, contra os ataques listados abaixo:

2.4.110.1. AJAX/JSON web threats;

2.4.110.2. Anonymous Proxy access

2.4.110.3. Application tampering;

2.4.110.4. Broken access control;

2.4.110.5. Buffer overflow;

2.4.110.6. Cross-site scripting (XSS);

2.4.110.7. Known Worms;

2.4.110.8. Malicious Encoding;

2.4.110.9. SQL injection;

2.4.110.10. Web Services (XML) attacks

2.4.110.11. XML bombs/DoS;

2.4.110.12. Brute force;

2.4.110.13. Cookie Injection;

2.4.110.14. Cookie manipulation;

2.4.110.15. Cookie poisoning;

2.4.110.16. Cross site request forgery (CSRF);

2.4.110.17. Directory Traversal;

2.4.110.18. Forceful browsing;

2.4.110.19. Hidden fields manipulation;

2.4.110.20. HTTP Denial of Service;

2.4.110.21. HTTP Response Splitting;

2.4.110.22. Illegal Encoding;

2.4.110.23. Layer 7 DoS and DDoS;

2.4.110.24. Malicious Robots;

2.4.110.25. OS Command Injection;

2.4.110.26. Parameter and HPP tampering;

2.4.110.27. Remote File Inclusion;

2.4.110.28. Request smuggling;

2.4.110.29. Sensitive data Exposure;

2.4.110.30. Session hijacking;

2.4.110.31. Web scraping;

2.4.110.32. Web server software and operating system attacks;

2.4.111. Deverá mitigar ataques de Slow HTTP;

2.4.112. A solução deve possuir lista dinâmica de endereços IP globais com atividades maliciosas;

2.4.113. A solução deve encriptar dados e credenciais na camada de aplicação, sem ter a necessidade de atualizar a aplicação;

2.4.114. Essas informações devem ser encriptadas para proteger o login e as credenciais dos usuários e com isso os dados da aplicação;

2.4.115. Deve ajudar a prevenir contra ataques de Credencial Stuffing, onde bases de credenciais expostas na Internet são usados para tentava de acesso de outras aplicações Web;

2.4.116. A solução deverá ser capaz de inspecionar e bloquear solicitações XML, SOAP e HTTP (versões HTTP 1.0, 1.1 e 2.0);

2.4.117. A solução deverá fazer checagem de:

2.4.117.1. Consistência de formulários;

2.4.117.2. Do cabeçalho do “user-agent” para identificar clientes inválidos; 4.131.3 Métodos HTTP utilizados (GET, POST, HEAD, OPTIONS, PUT, TRACE, DELETE, CONNECT), permitidos e bloqueados.

2.5. Gerenciamento

2.5.1. A solução deve ser gerenciada centralmente (configurações, controle e atualizações), através de interface web ou console de administração.

2.5.2. Possuir acesso controlado e autenticado por usuário, sendo que para a administração da solução deve-se usar uma conta para cada usuário administrador, independente da funcionalidade gerenciada.

2.5.3. O controle de acesso deve permitir a configuração de acesso por perfil às funções de Administração e Configuração de Regras.

2.5.4. Fornecer visualização e ações diferenciadas por perfis de acesso.

2.5.5. Permitir a visualização de painéis (dashboards).

2.5.6. Apresentar painéis gráficos (dashboards) com indicativos de situações diversas.

2.5.7. Deve possibilitar a CONTRATANTE, por meio do console de gerência, consultas sobre desempenho, problemas, configuração, mudanças e segurança do ambiente para cada domínio;

2.5.8. Deve armazenar as informações de desempenho do ambiente por um período mínimo de 30 (trinta) dias, mantendo estas informações disponíveis para a CONTRATANTE, sendo que o intervalo mínimo de coleta de informações dos elementos gerenciados deve ser de 05 (cinco) minutos, contendo no mínimo as seguintes informações:

2.5.8.1. Total de disponibilidade da Plataforma para um período mínimo 30 dias Por URL; Por conjunto de URL; Para todas as URL;

2.5.9. Deve possibilitar a geração de relatórios a qualquer tempo com as seguintes informações:

2.5.9.1. Total de GB (Gigabyte) consumido por domínio

2.5.9.2. Total de GB (Gigabyte) consumido no mês por todos os domínios;

2.5.9.3. Total de GB (Gigabyte) excedente, quando houver;

2.5.10. A solução deve permitir a emissão de relatórios gerenciais, conforme demanda da CONTRATANTE, com quantitativos e consumos por períodos;

2.5.11. A Plataforma deve possibilitar a consolidação de logs de toda a plataforma e seus recursos de forma global (todos os domínios) e individual (cada domínio) realizando seu armazenamento e retenção de forma segura;

2.5.12. Armazenar em log a identificação de tentativas de ataques e eventos gerados pela Plataforma e seus recursos, com no mínimo as seguintes informações:

2.5.12.1. Endereços IP que originaram os ataques;

2.5.12.2. Horário do ataque;

2.5.12.3. Nome do ataque;

2.5.12.4. Qual campo foi atacado;

2.5.12.5. Quantas vezes esse ataque foi realizado;

2.5.12.6. Técnicas utilizadas;

2.5.12.7. Eventos detectados que apontem:

2.5.12.8. Comportamentos maliciosos;

2.5.12.9. Comportamentos suspeitos;

2.5.12.10. Exploits;

2.5.12.11. Correlações de eventos;

2.5.12.12. Acessos;

2.5.13. Deve permitir, para toda a Plataforma e soluções que a compõem, a retenção de logs consolidados a cada 5(cinco) minutos por, no mínimo, 07(sete) dias;

2.5.14. Deve prover a retenção de logs detalhados por no mínimo 72 (setenta e duas) horas, para toda a Plataforma e soluções que a compõem;

2.5.15. Deve permitir que os logs sejam rotacionados de forma que os registros mais antigos sejam apagados quando não houver espaço de armazenamento disponível;

2.5.16. Deve possibilitar que por meio da console de gerência seja realizada a monitoração de logs e a investigação de logs;

2.5.17. Deve trabalhar com geolocalização para identificar a origem geográfica de um ataque;

2.5.18. Deve permitir exportar sob demanda os relatórios de logs em CSV;

2.5.19. Deve permitir o envio de logs para outros servidores de logs via syslog;

2.5.20. Deve permitir a configuração de alarmes personalizados, com base em investigações realizadas a partir dos logs;

2.5.21. Deve permitir apresentação dos dados consultados em vários formatos, incluindo tabela e gráficos;

2.5.22. Deve apresentar função de pesquisa por logs contendo no mínimo os seguintes critérios de pesquisa: Por dia, mês; Por domínio e endereço IP;

2.5.23. Deve permitir que sejam criados e aplicados filtros com base

em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, nome do ataque, o país de origem e destino;

2.5.24. Deve possibilitar a geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração; 5.25 Deve possibilitar a visualização do número de vezes que uma determinada regra foi usada (hits) em diferentes intervalos de tempo como dia, semana, mês ou intervalo customizável como data e horário de início e de fim da contagem; 5.26 Deve possibilitar a exportação de logs para fim de auditoria;

2.5.27. Possibilitar a exportação de logs para provedores de armazenamento compatíveis com S3;

2.5.28. Possibilitar a exportação de logs através de requisições HTTP para endpoints personalizados;

2.5.29. O equipamento deve fazer backup diário em forma automática de todas as informações nele armazenadas, incluindo as configurações de todos os módulos gerenciados e ter a capacidade de transferi-los automaticamente para um servidor remoto usando os protocolos SCP ou FTP;

2.5.30. Toda a configuração, administração e monitoramento da solução serão feitos através do console de administração;

2.5.31. A comunicação entre as estações de trabalho e o console de administração deve ser estabelecida através de um protocolo seguro com criptografia e autenticação por usuários locais, incluindo a possibilidade de usar certificados digitais;

2.5.32. A solução de administração deve permitir a atribuição de perfis de administração pelos usuários e esses perfis devem permitir a separação das funções de gerenciamento e monitoramento;

2.5.33. Capacidade de exportar logs para um formato SYSLOG ou SNMP TRAPS, para poder usar ferramentas de análise de terceiros;

2.5.34. O gerenciador deve possuir controle de interface gráfica Web (GUI: Graphical user interface) e interface por linha de comando (CLI – Command Line Interface);

2.5.35. A interface gráfica de gerenciamento deve ser cross-platform, em Web via protocolo HTTP e HTTPS, com suporte a acesso nativo via Microsoft Windows, Linux e Mac-OS;

2.5.36. Para interface gráfica do tipo Web, deve suportar no mínimo o navegador Mozilla Firefox e Chrome nas versões mais recentes;

2.5.37. A interface por linha de comando (CLI) deve possibilitar configuração dos equipamentos;

2.5.38. Deve possuir auto complementação de comandos;

2.5.39. Deve permitir acesso via SSH, criptografado;

2.5.40. Possuir um comando que mostre o tráfego de utilização das interfaces (bps e/ou pps);

2.5.41. Permitir reinicialização do equipamento;

2.5.42. Implementar Debugging: CLI via console e SSH;

2.5.43. A solução de gerenciamento deve possuir, no mínimo, três

níveis de usuários: Administrador; Usuário com permissões reduzidas; e usuário Somente Leitura;

2.5.44. A solução de WAF e a solução de balanceamento de carga entre aplicações web do TRF6 deverão permitir que mais de um usuário possa estar conectado simultaneamente a interface de administração com a permissão de leitura/escrita;

2.5.45. A solução não deverá ter nenhum limite de licença para a quantidade de usuários ou dispositivos que poderão ser configurados. O único limite que será permitido é de capacidade do processamento dos appliances dentro dos throughputs e quantidade de requisições solicitados;

2.5.46. Deverá permitir autenticação dos usuários em bases remotas como, no mínimo, Microsoft Active Directory, RADIUS e OpenLDAP;

2.5.47. A interface gráfica de gerenciamento deverá permitir a atualização do sistema operacional e/ou a instalação de patches ou Hotfixes sem o uso da linha de comando;

2.5.48. Utilizar SCP ou HTTPS como mecanismo de transferência de arquivos de configuração e Sistema Operacional;

2.5.49. A interface Gráfica deverá permitir a reinicialização do equipamento;

2.5.50. A Solução de gerenciamento deve possuir uma única console que permita a organização, gerenciamento, configuração e aplicação das políticas de segurança, regras de balanceamento, aceleração, cache em todos os equipamentos que compõem a solução de WAF com balanceamento;

2.5.51. A Gerência deve ter capacidade de obter e analisar eventos em tempo real;

2.5.52. A Solução de gerenciamento deve fornecer as seguintes funcionalidades no seu ambiente gráfico:

2.5.52.1. Adição, alteração ou remoção de aplicações a serem protegidas pelo firewall de proteção a aplicações Web;

2.5.52.2. Adição, alteração ou remoção de regras de balanceamento, aceleração e cache;

2.5.52.3. Obter e analisar eventos em tempo real e gerar relatórios durante a avaliação do tráfego;

2.5.52.4. Permitir utilizar as informações obtidas para refinar as políticas de segurança a qual gerou o evento;

2.5.52.5. Permitir a criação de listas de acesso baseadas em endereços IP. Deve ser possível definir os endereços IP de origem das sessões.

2.5.53. Deve manter internamente múltiplos arquivos de configurações do sistema;

2.5.54. Deve permitir a exportação e importação de regras e políticas para um novo dispositivo de forma simples;

2.5.55. Deve permitir o armazenamento de sua configuração em memória não volátil, no caso de uma queda e posterior restabelecimento da alimentação, voltar à operação normalmente na

mesma configuração anterior à queda de alimentação;

2.5.56. Deve suportar rollback de configuração e imagem;

2.5.57. Deve possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, traceroute, ping e log de eventos;

2.5.58. O sistema operacional do dispositivo deverá permitir a utilização da ferramenta tcpdump, ou similar de qualidade igual ou superior, para captura e monitoração de pacotes em quaisquer de suas interfaces de rede, permitindo que as capturas sejam armazenadas em formato libpcap;

2.5.59. A execução do tcpdump, ou ferramenta similar, não deve impactar no desempenho dos appliances. Permitir a definição de funcionalidades e dados requeridos por auditores;

2.5.60. O armazenamento dos demais dias poderá ser local ou remoto;

2.5.61. Possuir configuração de múltiplos syslog servers para os quais o equipamento irá enviar as mensagens de syslog;

2.5.62. Possuir agente de gerenciamento SNMP, MIB SNMP II, extensões MIB SNMP, MIB bridging (RFC 1493), que possua descrição completa da MIB implementada no equipamento, inclusive as extensões privadas, se existirem;

2.5.63. Suporte ao protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol).

2.6. Capacitação Técnica

2.6.1. O treinamento deverá ser completo para contemplar a instalação, customização, operação e administração da solução de WAF para 5 (cinco) funcionários da CONTRATANTE, na modalidade de Ensino a Distância (EAD), online e ao vivo;

2.6.2. O treinamento deverá ser ministrado para turma especifica para a CONTRATANTE;

2.6.3. Serão aceitos cursos oficiais do fabricante da solução;

2.6.4. Deverá possuir módulos teóricos e práticos;

2.6.5. Os instrutores devem ser certificados pelo fabricante da solução para o treinamento;

2.6.6. O conteúdo dos cursos deverá abranger, minimamente, os seguintes tópicos:

2.6.6.1. Configuração – acesso e navegação na solução; comando de configurações básicas e avançadas; estrutura/arquitetura do sistema operacional dos equipamentos; configuração via CLI, GUI, Client e web;

2.6.6.2. Operação e troubleshooting avançado – comandos de gerenciamento e monitoramento da saúde dos recursos dos equipamentos; aplicação de bloqueios manuais e automáticos e criação de filtros;

2.6.7. É obrigatório relacionar a ementa dos cursos, carga horária e conteúdo programático. A abordagem do treinamento deve ser eminentemente prática, utilizando exemplos e exercícios para ilustrar os conceitos e capacitar os participantes a empregar os recursos oferecidos;

2.6.8. Ao final do treinamento deve ser emitido certificado de conclusão para cada participante/aluno constando a carga horária e a ementa

2.7. Software e Licenciamento

2.7.1. Todas as licenças que compõem a solução deverão ser de propriedade da CONTRATANTE e permitir a plena continuidade de utilização e operação da solução mesmo após o término do contrato, de forma perpétua.

2.7.2. As assinaturas da solução de WAF devem ser atualizadas durante o período do contrato sem que seja necessário nenhum custo adicional por parte da CONTRATANTE na aquisição de novas licenças ou subscrições.

2.8. Instalação e Configuração

2.8.1. O serviço de instalação e configuração deverá ser executado por técnico certificado pelo fabricante;

2.8.2. O serviço de instalação compreende as atividades de planejamento, instalação física, instalação lógica e finalização da solução no ambiente da CONTRATADA;

2.8.3. O serviço de configuração consiste em ajustar todos os parâmetros necessários (físicos e lógicos) para o funcionamento da solução e a sua adequação para funcionamento no ambiente da CONTRATADA atendendo aos requisitos dessa especificação.

2.9. Operação Assistida

2.9.1. A operação assistida deverá ocorrer durante 45 (quarenta e cinco) dias corridos a partir da instalação e configuração da solução na CONTRATANTE;

2.9.2. O serviço de operação assistida é composto por um conjunto de atividades que permitem o treinamento e a capacitação da equipe da CONTRATANTE responsável pelas atividades de operação, manutenção preventiva e corretiva, transferindo todo o conhecimento e experiência necessária para a operação da solução;

2.9.3. Durante os 45 dias corridos, será prestado todo o suporte necessário para a operacionalidade da solução, minimizando o risco da implantação da solução e proporcionando as condições ideais para transferência da tecnologia envolvida em regime de treinamento enquanto trabalha, até que a CONTRATANTE possa assumir as atividades com sua própria equipe;

2.9.4. Durante a operação assistida também será necessário realizar, pela CONTRADADA, possíveis customizações e ajustes finais que forem identificados durante o período de instalação, configuração e operação assistida;

2.9.5. Por padrão, a prestação da operação assistida ocorrerá presencialmente nas dependências da CONTRATANTE ou remotamente a ser definido pela CONTRATANTE.

2.10. Suporte, Manutenção e Atualização de Versão

2.10.1. O suporte técnico compreende o diagnóstico e identificação de problemas, apoio técnico na utilização, correção de erros, defeitos

(bugs) ou mau funcionamento sobre qualquer funcionalidade, recurso, componente ou módulo disponível de forma nativa na solução de WAF e balanceamento, ou decorrente de qualquer adaptação (customização) e ajuste (tuning) efetuada pela CONTRATANTE;

2.10.2. O atendimento a um chamado de suporte deverá ocorrer por qualquer uma das seguintes formas: contato telefônico, envio de mensagem eletrônica (e-mail), acesso ao sítio (website) da CONTRATADA ou do fabricante da solução de WAF, com controle de acesso por senha;

2.10.3. O atendimento telefônico sempre que aplicável e viável, por meio de ligação local em Belo Horizonte/MG ou ligação interurbana gratuita (0800) e deverá ter um único número de contato para todos os produtos de software que compõem a solução de WAF;

2.10.4. A CONTRATANTE poderá efetuar um número ilimitado de chamados técnicos para a CONTRATADA, por qualquer uma das formas disponíveis, durante vigência do contrato vinculado a este edital;

2.10.5. Na abertura ou registro de um chamado técnico, por qualquer uma das formas disponíveis, a CONTRATADA deverá informar: data e hora de abertura do chamado, descrição do chamado, nível de severidade do chamado e identificação completa do solicitante;

2.10.6. A CONTRATADA deverá retornar, via e-mail, a confirmação da abertura do chamado técnico, doravante denominado confirmação do chamado, contemplando as seguintes informações na sua abertura: código de identificação do chamado, identificação do responsável da CONTRATADA pela abertura do chamado;

2.10.7. O atendimento ao chamado técnico pela CONTRATADA deverá ocorrer pelo menos por uma das seguintes formas: chamada telefônica, envio de mensagem eletrônica (e-mail), recursos disponíveis no sítio (site) do fabricante da solução de WAF ou da CONTRATADA, presencial ou suporte por acesso remoto;

2.10.8. Caso acionado o suporte direto do fabricante, este deverá ter atendimento em português. Caso contrário, a CONTRATADA deverá ser responsável por intermediar os contatos entre o fabricante e a CONTRATANTE;

2.10.9. Um chamado técnico somente será considerado contingenciado ou concluído com o aceite da CONTRATANTE, na forma de um visto na ordem de serviço correspondente ou aceite por e-mail ou ainda, diretamente no sistema oferecido pela CONTRATADA, caso esta forma seja utilizada;

2.10.10. Após apresentar uma solução de contorno para o chamado técnico, a CONTRATADA deverá retornar, via e-mail, a confirmação da execução do serviço, contemplando as seguintes informações: código de identificação do chamado, data e hora de conclusão do atendimento, descrição dos serviços executados e/ou da solução apresentada;

2.10.11. Em caso de adoção de solução de contorno, sem prejuízo da solução definitiva cabível, a CONTRATADA deverá emitir laudos, na periodicidade exigida pela CONTRATANTE, informando sobre a evolução dos trabalhos para solucionar o problema de forma

definitiva;

2.10.12. Após apresentar uma solução definitiva para o CHAMADO TÉCNICO, a CONTRATADA deverá retornar, via e-mail, a confirmação da execução do serviço, contemplando as seguintes informações: código de identificação do chamado, data e hora de conclusão do atendimento, descrição dos serviços executados e/ou da solução apresentada;

2.10.13. Deverá ser garantido à CONTRATANTE o pleno acesso ao sítio (site) dos fabricantes dos produtos que compõem a solução de WAF, com direito a consultas a quaisquer bases de conhecimentos e fóruns de discussão disponíveis para seus usuários;

2.10.14. Caberá exclusivamente à CONTRATANTE a decisão de implantar ou não quaisquer atualizações de software fornecidos pela CONTRATADA;

2.10.15. A CONTRATADA deverá disponibilizar mecanismos para a atualização de software pelo download direto através da própria aplicação, pelo envio das mídias ou através de download no seu sítio (site) ou do fabricante do software em questão;

2.10.16. O serviço de manutenção consiste na correção de qualquer problema ou falha apresentados em componentes físicos ou lógicos da solução;

2.10.17. A atualização de software é uma alteração da versão anterior com o objetivo de implementar melhorias. Essas melhorias podem ser de usabilidade, correção de falhas, desempenho, adição de novas funcionalidades, etc.;

2.10.18. O prazo de atualização de todo software fornecido deve ser igual ao período de garantia do produto. Durante a vigência do contrato, a CONTRATANTE terá direito a todas atualizações de versão e release dos softwares.

2.11. Garantia

2.11.1. O(s) equipamento(s) que compõe(m) a solução devem estar em sua versão mais atual até a data de assinatura do contrato e a data de final de suporte (end-of-support) deve ocorrer após o término da vigência contratual da solução;

2.11.2. O serviço de Garantia contempla garantir o correto e pleno funcionamento de todos os itens adquiridos necessários para o funcionamento da solução, incluindo atualizações regulares de segurança e patches para proteger contra novas vulnerabilidades e ameaças;

2.11.3. Prazo de garantia deverá ser de 60 meses.

3. LOTE 3. SERVIÇO DE SEGURANÇA DE BORDA (SERVICE SECURITY EDGE - SSE)

3.1. Características Gerais da Solução

3.1.1. O SSE deve possuir os seguintes componentes:

3.1.1.1. Acesso à Rede Zero Trust (ZTNA): O ZTNA;

3.1.1.2. Agente de segurança de acesso à nuvem (CASB);

3.1.1.3. Gateway seguro da web (SWG).

3.1.2. A solução deve ser fornecida com licenças para 4500 usuários, com validade de 60 meses, incluindo todas as funcionalidades e atualizações necessárias durante o período de assinatura a fim de assegurar o acesso à internet e a aplicativos para usuários remotos;

3.1.3. A solução deve ser construída com uma arquitetura nativa em nuvem e entregue como um serviço (SaaS), garantindo alta disponibilidade, escalabilidade e manutenção contínua sem interrupções significativas para os usuários finais;

3.1.4. O serviço deve possuir infraestrutura de filtragem web (proxy) em datacenter localizado no território brasileiro, sendo permitida a replicação desta infraestrutura em outros países;

3.1.5. A inspeção do conteúdo de conexões originadas no Brasil deve ser feita em datacenter dentro do território brasileiro;

3.1.6. Visando a disponibilidade e redundância do serviço, a CONTRATADA deverá oferecer em sua plataforma, pelo menos, 2 (dois) datacenters em território brasileiro;

3.1.7. Todas as funcionalidades deverão ser ofertadas na nuvem como serviço. A nuvem deverá ser distribuída globalmente, incluindo o Brasil, e deverá ser licenciada para, pelo menos, 4.500 (quatro mil e quinhentos) usuários;

3.1.8. A solução deverá prover no mínimo 2 (dois) endereços exclusivos para TRF6 (/31) para acesso à Internet por datacenter no Brasil, de forma a garantir a saída por apenas com IPs designados para os Datacenters posicionados no Brasil;

3.1.9. O datacenter localizado no Brasil deverá ter conectividade redundante ao PTT (Ponto de Troca de Tráfego) no Brasil, peering estabelecido com provedores de serviços, empresas de telecomunicações, CDNs (Content Delivery Network) e provedores de nuvem pública tais como (AWS, Microsoft e Google). Desta forma, será possível garantir melhor experiência e baixa latência aos usuários;

3.1.10. O datacenter do fabricante localizado no Brasil deve possuir, no mínimo, 2 (dois) links com velocidade superior a 50Gbps no principal ponto de troca do Brasil (IX.BR);

3.1.11. O fabricante deve possuir infraestrutura em território brasileiro.

3.1.11.1. Admite-se a hospedagem em datacenter de nuvem pública estabelecida no Brasil.

3.1.12. O datacenter do fabricante localizado em território nacional não deve armazenar as informações das transações em disco local. Os dados referentes as transações devem ser compactados, tokenizados e exportados para uma estrutura apartada de armazenamento de logs, que deverá ser prevista nesta contratação, através de conexões TLS seguras.

3.1.13. Não serão aceitos sistemas baseados em hardware ou software projetados para uso genérico, ou de código aberto (*open source*);

3.1.13.1. Os elementos ofertados não podem ser customizados.

3.1.14. A solução deve oferecer uma interface de administração centralizada e intuitiva, permitindo o gerenciamento eficiente das

políticas de segurança, configurações de usuários e análise de relatórios de acesso e autenticação;

3.1.15. O serviço deve garantir a disponibilidade mensal mínima de 99,7%, assegurando-se a máxima confiabilidade e tempo de atividade do sistema;

3.1.16. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

3.1.17. Deve consolidar múltiplos serviços de segurança para controle de acesso à Internet, como DNS, Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Remote Browser Isolation (RBI);

3.1.18. O agente instalado deve ser capaz de identificar quando estiver conectado à internet de maneira remota, ou por dentro da infraestrutura do escritório remoto. Para com isso ser ativado/desativado de acordo com a política.

3.1.19. A solução não deve depender de cliente instalado na máquina do usuário. Para o acesso agentlesss, deve suportar, no mínimo, os seguintes tipos de aplicações:

3.1.19.1. Web;

3.1.19.2. SSH;

3.1.19.3. RDP.

3.1.20. Toda a comunicação entre o usuário e a plataforma deve ser realizada através de conexões TLS;

3.1.21. Deve ser compatível os seguintes provedores de identidade: Okta, Azure AD ou Active Directory / LDAP; SAML 2.0 Identity Providers; Auth0, Google Workspace e Workday;

3.1.22 Deve possuir base de inteligência do próprio fabricante, que inclua recursos de Inteligência Artificial (IA), estatística e modelos de aprendizado de máquina para fornecer informações sobre ameaças de cibersegurança ameaças e melhorar as taxas de resposta a incidentes;

3.1.23. A solução deve permitir a implementação de respostas automáticas ou guiadas a incidentes, minimizando o impacto de ameaças detectadas;

3.1.24. A solução deve oferecer integração rápida com plataformas de comunicação como Slack e Microsoft Teams, facilitando a notificação imediata de incidentes;

3.1.25. Deve ser compatível com plataformas de Information Event Management (SIEM) e Security Orchestration, Automation and Response (SOAR), permitindo uma análise de segurança aprofundada e resposta automatizada a incidentes;

3.1.26. O portal deve ser uma extensão da solução de Single Sign-On, permitindo que os usuários entrem uma única vez e obtenham acesso a todas as aplicações autorizadas sem a necessidade de autenticações adicionais devendo também permitir a configuração de login único (SSO) para acesso através da integração com um provedor de identidade (IdP) compatível com SAML 2.0 Identity Providers, Okta, AzureAD, Active Directory / LDAP, Google Workspace.

3.1.27. A validação de postura para máquinas Windows deve

contemplar pelo menos a validação de:

3.1.27.1. Antivírus instalado;

3.1.27.2. Certificados;

3.1.27.3. Processos em execução;

3.1.27.4. Versão de SO.

3.1.28. A validação de postura também deverá se aplicar ao acesso *agentless* (sem agentes), não apenas ao acesso com cliente instalado no dispositivo do usuário.

3.1.29. A validação de postura para o acesso agentless deve contemplar no mínimo as seguintes validações:

3.1.29.1. Data e hora de acesso;

3.1.29.2. IP;

3.1.29.3. Localização (País de acesso);

3.1.29.4. SO.

3.1.30. O client deve estar disponível para os seguintes Sistemas Operacionais:

3.1.30.1. Windows (.exe e .msi);

3.1.30.2. Linux;

3.1.30.3. Android / Chromebook;

3.1.30.4. iOS;

3.1.30.5. Na falta do agente, admite-se o acesso *agentless* via portal web.

3.2. Módulo de Gerenciamento

3.2.1. Deve prover console em nuvem, para todas as funções próprias da solução sendo aceita composição de solução do mesmo fabricante;

3.2.2. Deve permitir extrair logs a partir de soluções externas, como SIEM;

3.2.3. Deve possuir autenticação via protocolo SAML, permitindo integrar com provedores de serviços de identidade (IdP) para acesso administrativo à console;

3.2.4. Deve suportar APIs para gerenciamento com, no mínimo, as seguintes funcionalidades:

3.2.4.1. Autenticação;

3.2.4.2. Provisionamento;

3.2.4.3. Gestão de Políticas;

3.2.4.4. Relatórios.

3.2.5. Deve possuir ao menos três níveis de usuário: Administrador completo, Administrador de segurança e Apenas leitura;

3.2.6. Prover painel com informações sumarizadas de navegação de usuários contendo quantidade de sessões ativas e consumo de banda através de uma linha do tempo;

3.2.6.1. A gerência centralizada e monitoração deve possibilitar a

visualização dos logs de Firewall, navegação web e prevenção de ameaças;

3.2.6.2. Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento.

3.3. Segurança de Acesso - Política de Acesso

3.3.1. Deve usar o conceito de política de acesso unificada, sem políticas separadas para DNS, Secure Web Gateway (SWG);

3.3.2. Deve permitir ações de Bloqueio, Permissão, Alerta e Isolamento (Remote Browser Isolation);

3.3.3. Deve permitir a criação de páginas personalizadas de bloqueio e alerta, com opção de contato com administrador;

3.3.4. Deve permitir especificar origens a serem usadas na política de acesso internet, com base em:

3.3.4.1. Usuários/Grupos através de integração com Microsoft Active Directory ou provedores de identidade via SAML, tais como Azure AD e Okta;

3.3.5. Deve permitir especificar destinos a serem usados na política de acesso internet, com base em:

3.3.5.1. Listas personalizadas de domínios, URLs, IPs/Redes, incluindo a capacidade de fazer o upload destas;

3.3.5.2. IP/Redes, Portas e Protocolos (Any, UDP, TCP, ICMP);

3.3.5.3. Categorias de conteúdo web ou listas personalizadas de categorias.

3.3.5.4. Aplicações ou listas personalizadas de aplicações.

3.3.6. Deve aplicar uma regra de acesso internet padrão e customizável, caso o fluxo não seja mapeado em outra regra;

3.3.7. Deve possuir contador de visitas (Hit count), indicando quantas vezes uma regra foi acionada.

3.4. Segurança de Acesso Internet - Camada DNS

3.4.1. Deve possuir infraestrutura global de resolução recursiva de DNS para proteção de acesso à internet;

3.4.2. Não deve ser uma solução para configuração, manutenção, implementação e serviço de DNS autoritativo;

3.4.3. Não deve ser uma solução para substituição de infraestrutura DNS interno, serviço DHCP;

3.4.4. Deve oferecer proteção para dispositivos de rede internos e externos;

3.4.5. Deve possuir suporte a IPv6 para DNS;

3.4.6. Deve permitir os seguintes métodos de envio de tráfego DNS:

3.4.6.1. Integração nativa com o sistema de DNS atual do ambiente de produção, substituindo as referências de servidores recursivos externos em uso.

3.4.7. Deve permitir visibilidade e controle de acesso a domínios, por

meio de classificação por categorias;

3.4.8. Deve permitir a definição de listas personalizadas de acesso a domínios, para permissão (allow lists) e para bloqueio (block lists) incluindo a capacidade de fazer o upload destas;

3.4.9. Deve ser capaz de identificar e bloquear requisições de acesso a domínios que estejam classificados, no mínimo, nas categorias de segurança abaixo:

3.4.9.1. Malware;

3.4.9.2. Command and Control (C&C);

3.4.9.3. Phishing;

3.4.9.4. DNS dinâmico;

3.4.9.5. Cryptomining;

3.4.9.6. Domínios novos ou vistos pela primeira vez, por, no mínimo, 24h;

3.4.9.7. DNS Tunneling;

3.4.9.8. Domínios suspeitos ou potencialmente maliciosos.

3.5. Gateway Seguro da Web - Secure Web Gateway (SWG)

3.5.1. A solução deverá identificar automaticamente tráfegos Web em portas não padrão (80 e 443) e realizar a inspeção Web completa, incluindo inspeção SSL e todas as funcionalidades de controle de acesso e segurança, mesmo em uma arquitetura de proxy transparente.

3.5.2. Deve permitir visibilidade e controle de acesso a URLs, por meio de classificação por categorias;

3.5.3. Deve permitir visibilidade e controle de acesso a URLs não categorizadas pelo fabricante;

3.5.4. Deve permitir a definição de listas personalizadas de acesso a domínios, URLs e IPs, para permitir (allow lists) e para bloqueio (block lists) incluindo a capacidade de fazer o upload destas;

3.5.5. Deve suportar descriptografia TLS/HTTPS completa ou seletiva, com suporte a Certificate Authority (CA) do próprio cliente;

3.5.6. Deve permitir excluir categorias de conteúdo, aplicações e domínios do processo de descriptografia (descriptografia seletiva);

3.5.7. Deve suportar descriptografia e inspeção de TLS 1.2 e 1.3;

3.5.8. Deve possuir recurso de antivírus/anti-malware para escaneamento de arquivos em trânsito;

3.5.9. Deve possuir mecanismo automático de envio de arquivos para malware sandboxing;

3.5.10. Deve permitir os seguintes métodos de envio de tráfego Secure Web Gateway(SWG):

3.5.10.1. Arquivo PAC (Proxy Auto-Configuration);

3.5.10.2. Túnel Ipsec;

3.5.10.3. Encaminhamento de tráfego com cliente para máquinas windows, macOS, linux e android;

3.5.11. Deve possuir controle granular (Upload e/ou Download) de aplicações web, suportando ao menos:

3.5.11.1. Box;

3.5.11.2. X (Twitter);

3.5.11.3. Dropbox;

3.5.11.4. Pinterest;

3.5.11.5. Messenger;

3.5.11.6. Gmail;

3.5.11.7. Facebook;

3.5.11.8. Linkedin;

3.5.11.9. Slack;

3.5.11.10. Instagram;

3.5.11.11. Google Drive;

3.5.11.12. SlideShare;

3.5.11.13. YouTube;

3.5.11.14. Vimeo;

3.5.11.15. WhatsApp;

3.5.11.16. SmartSheet;

3.5.11.17. Pastebin;

3.5.11.18. WeTransfer.

3.6. Agente de segurança de acesso à nuvem (CASB):

3.6.1. Deve ser capaz de monitorar a utilização de serviço em nuvem (Cloud Services) para identificar riscos e desenvolver atividades de conformidade (Shadow IT);

3.6.2. Deve possuir relatórios sobre a categoria do fornecedor, nome do aplicativo e volume de atividade para cada aplicativo descoberto;

3.6.3. Deve incluir detalhes do aplicativo e informações de risco, como pontuação de reputação na Web, viabilidade financeira e certificações de conformidade relevantes;

3.6.4. Deve possuir capacidade de bloquear/permitir aplicativos específicos;

3.6.5. Deve possuir recurso de detecção, quarentena e/ou remoção de malware em aplicativos baseados em nuvem, via API, no mínimo para os seguintes aplicativos:

3.6.5.1. Dropbox;

3.6.5.2. Box;

3.6.5.3. Webex Teams;

3.6.5.4. Microsoft 365;

3.6.5.5. Google Drive.

3.6.6. Deve possuir opção de restrições de locatário (Tenant Controls) para permitir acesso apenas a instâncias de aplicativos SaaS indicados pelo administrador, suportando, no mínimo, os seguintes aplicativos:

3.6.6.1. Microsoft 365;

3.6.6.2. Google G Suite;

3.6.6.3. Slack;

3.6.6.4. Dropbox.

3.7. Remote Browser Isolation (RBI)

3.7.1. Deve possuir funcionalidade de isolamento remoto de browser para proteção contra potenciais ameaças e malware, através do direcionamento do tráfego HTTPS a um serviço de browser protegido em nuvem;

3.7.2. A funcionalidade de RBI deve ser acionada como opção de ação a ser tomada nas regras para destinos e identidades selecionados;

3.7.3. A funcionalidade de RBI deve poder ser acionada para destinos considerados arriscados, como sites não categorizados e categorias de ameaça de segurança;

3.7.4. A funcionalidade de RBI deve poder ser acionada para qualquer destino, categoria ou aplicação suportada pelo serviço de proxy;

3.7.5. O RBI deve suportar os seguintes navegadores:

3.7.5.1. Apple Safari;

3.7.5.2. Google Chrome;

3.7.5.3. Microsoft Edge;

3.7.5.4. Mozilla Firefox.

3.7.6. O RBI deve suportar autenticação de terceiros (ex. Dropbox usando Google para autenticação).

3.8. Data Loss Prevention (DLP)

3.8.1. Deve possuir camada múltipla de DLP para dados em trânsito (em tempo real) e em repouso (via API);

3.8.2. Deve permitir a classificação de dados sensíveis através de uso individual ou combinado de dicionários pré- definidos e personalizados;

3.8.3. Deve permitir a classificação de dados sensíveis através de dicionários personalizados com opção de termos, frases e padrões via expressões regulares;

3.8.4. Deve permitir configurar diferentes níveis de severidade por regra;

3.8.5. Deve permitir inspecionar os arquivos por nome, conteúdo ou ambos;

3.8.6. O DLP deve suportar, no mínimo, os seguintes tipos de arquivos:

3.8.7.1. Word .doc e .docx;

3.8.7.2. PDF;

3.8.7.3. RTF;

3.8.7.4. Excel .xls e .xlsx;

3.8.7.5. PowerPoint .ppt e .pptx;

3.8.7.6. OpenDocument presentation .odp;

3.8.7.7. OpenDocument sheet .ods;

3.8.7.8. OpenDocument word .oth;

3.8.7.9. E-mail;

3.8.7.10. CSV;

3.8.7.11. HTML/XML;

3.8.7.12. Texto .txt;

3.8.7.13. TSV;

3.8.7.14. URL.

3.8.8. O DLP para dados em trânsito deve ter opções de alerta e bloqueio para dados expostos em arquivos, formulários web e aplicações web;

3.8.9. O DLP para dados em trânsito de suportar os seguintes tipos de formulários (forms):

3.8.9.1. JSON;

3.8.9.2. XML;

3.8.9.3. URL encoded;

3.8.9.4. Multipart form.

3.8.10. O DLP para dados em trânsito deve ter, no mínimo, os seguintes serviços para inspeção:

3.8.10.1. Box Cloud Storage;

3.8.10.2. ChatGPT;

3.8.10.3. Concur Invoice;

3.8.10.4. Confluence;

3.8.10.5. Dropbox;

3.8.10.6. Facebook Messenger;

3.8.10.7. Gmail;

3.8.10.8. Jira;

3.8.10.9. Linkedin SlideShare;

3.8.10.10. Monday;

3.8.10.11. PasteBin;

3.8.10.12. SalesForce;

3.8.10.13. ServiceNow;

3.8.10.14. ShareFile;

3.8.10.15. Slack;

3.8.10.16. SmartSheet;

3.8.10.17. WeTransfer;

3.8.10.18. WorkDay;

3.8.10.19. Yahoo Mail.

3.8.11. Deve permitir especificar as identidades a serem usadas na política de DLP de dados em trânsito, com base em:

3.8.12. O DLP para dados em repouso deve permitir varredura de arquivos compartilhados, pelo menos, nas seguintes aplicações:

3.8.12.1. Microsoft 365 OneDrive e Sharepoint;

3.8.12.2. Google Drive.

3.8.13. O DLP para dados em repouso deve dar opções de ação de monitorar e revogar acesso;

3.8.14. O DLP para dados em repouso deve permitir especificar o escopo de varredura para todos os usuários ou usuários específicos.

3.9. Acesso à Rede Zero Trust (ZTNA)

3.9.1. Deve usar o conceito de política de acesso unificada, sem políticas separadas para ZTNA;

3.9.2. Deve permitir ações de Bloqueio e Permissão;

3.9.3. Deve permitir especificar origens a serem usadas na política de acesso privado, com base em:

3.9.3.1. Usuários/Grupos através de integração com Microsoft Active Directory ou provedores de identidade via SAML, tais como Azure AD e Okta.

3.9.4. Deve permitir especificar destinos a serem usados na política de acesso a recursos privados, com base em:

3.9.4.1. Aplicações internas previamente configuradas, de forma individual ou global.

3.9.5. Deve permitir especificar requisitos de dispositivo de origem a serem usadas na política de acesso privado, com base em:

3.9.5.1. Postura do dispositivo gerenciado ou não conforme política;

3.9.5.2. Requisitos de autenticação recorrente de usuário.

3.9.6. Deve aplicar uma regra padrão que negue acesso privado, caso o fluxo não seja mapeado em outra regra;

3.9.7. Deve possuir contador de visitas (Hit count), indicando quantas vezes uma regra foi acionada;

3.9.8. Deve permitir habilitar e desabilitar regras individualmente;

3.9.9. Suportar descriptografia para inspeção de tráfego privado.

3.10. Conector de recursos privados do ZTNA

3.10.1. A solução deve possibilitar conexões rápidas e seguras a redes e aplicações privadas, por meio de máquinas virtuais (VMs) implantadas à frente das aplicações privadas, que forneçam conectividade de dentro para fora. Deve ser possível instalar nos ambientes:

3.10.1.1. On-premises através de uma imagem VMWare ESXi (ova);

3.10.1.2. Nuvem AWS;

3.10.1.3. Nuvem Azure;

3.10.1.4. Nuvem Google.

3.10.2. Deve ter a capacidade de suportar conexão DTLS e TLS;

3.10.2.1. Deve regredir para a conexão TLS, caso DTLS seja bloqueado;

3.10.3. Deve ter a capacidade de calcular o número de instâncias baseado no throughput de tráfego estimado;

3.11. ZTNA com Agente

3.11.1. Deve ter a capacidade de acessar recursos privados utilizando qualquer protocolo;

3.11.2. Deve permitir a aplicação de políticas de postura do usuário, incluindo os seguintes requisitos:

3.11.2.1. Verificação do sistema operacional e a versão;

3.11.2.2. Verificação de um agente de segurança no dispositivo;

3.11.2.3. Verificação de senha no dispositivo;

3.11.2.4. Verificação do navegador utilizado e sua versão.

3.11.3. Deve rotear o tráfego baseado no IP/FQDN da aplicação destino;

3.12. ZTNA sem Agente (via browser)

3.12.1. Deve ser possível acessar aplicações privadas sem agente instalado;

3.12.2. Deve ter a capacidade de gerar um FQDN resolvível publicamente;

3.12.3. Deve ter a capacidade de autenticação via SAML;

3.12.4. Deve ter a capacidade de prover conexão a recursos privados para dispositivos não gerenciados BYOD;

3.12.5. Deve ter a capacidade de selecionar os navegadores permitidos;

3.12.6. Deve ter a capacidade de selecionar os sistemas operacionais permitidos.

3.13. Painéis e Relatórios

3.13.1. Deve possuir painel de visão geral do ambiente, incluindo informações de, pelo menos:

3.13.1.1. Gráfico com volume de tráfego (total, enviado e recebido) agregado e por método de conexão no período selecionado;

3.13.1.2. Atividade de segurança (solicitações e bloqueios) e principais categorias de segurança visitadas por dispositivos e usuários no período selecionado;

3.13.1.3. Conexões de rede privada ZTNA ao longo do tempo, listando usuários com maior número de solicitações no período selecionado;

3.13.1.4. Número de vezes que os aplicativos internos foram acessados, número de usuários que solicitaram acesso e o número de solicitações permitidas ou bloqueadas durante o período selecionado;

3.13.1.5. Número de vezes que cada método de acesso (ZTNA

com cliente, ZTNA sem cliente) foi utilizado e recursos internos mais utilizados no período selecionado.

3.13.2. Deve prover, no mínimo, os seguintes relatórios:

3.13.2.1. Todas as atividades de acesso durante um determinado período de tempo ajustável, relacionadas a segurança ou não, com filtros, no mínimo, por tipo de evento, camada responsável pela detecção, ação tomada, identidade usada no acesso, destino, categoria de segurança e categoria de conteúdo;

3.13.2.2. Todas as atividades de acesso relacionadas a segurança durante um determinado período de tempo ajustável, com filtros, no mínimo, por tipo de evento, ação tomada, identidade usada no acesso, destino e categoria de segurança;

3.13.2.3. Visão sobre aplicativos Web descobertos (Shadow IT), indicando fornecedor, categoria, nome, volume de atividade, risco, certificações de conformidade relevantes e identidades usadas nos acessos;

3.13.2.4. Destinos mais acessados num período determinado de tempo ajustável, relacionados a segurança ou não, com filtros, no mínimo, por camada responsável pela detecção, ação tomada, identidade usada no acesso,

categoria de segurança e categoria de conteúdo;

3.13.2.5. Categorias mais acessadas num período determinado de tempo ajustável, relacionadas a segurança ou não, com filtros, no mínimo, por camada responsável pela detecção, ação tomada e identidade usada no acesso;

3.13.2.6. Atividades executadas na console da solução, indicando usuário responsável, data e hora, IP de origem, área do produto relacionada e ação executada, com possibilidades de filtro, no mínimo, por usuário, período de

tempo e IP;

3.13.2.7. Visão geral dos arquivos maliciosos identificados nas plataformas SaaS integradas ao ambiente, indicando total de arquivos escaneados, total de malwares detectados, total de usuários com malware, data e hora da detecção, com filtros, no mínimo, por plataforma, nível de exposição, status e nome do arquivo. Deve possibilitar ações de isolar em quarentena e restaurar arquivos;

3.13.2.8. Violações de dados (DLP) detectadas em tempo real e via API, indicando data e hora do evento, regra acionada, identidade envolvida, nome do arquivo e URL de destino, com filtros, no mínimo, por tipo (real time ou API), ação tomada, severidade, aplicação, nível de exposição, identidade e hash de arquivos. Deve indicar, nos detalhes do evento, trecho do conteúdo de texto exposto que acionou a regra, com as devidas máscaras para a parte mais sensível do texto.

3.13.3. Todos os dados disponíveis para a consulta e criação de relatórios deverão residir no plano de gestão por, no mínimo, 30 dias;

3.13.4. Deve permitir exportar relatórios para arquivos CSV, JSON, HTML ou outro formato capaz de manipulação;

3.13.5. Deve permitir agendamento e envio automático de relatórios.

3.14. Monitoramento de Experiência Digital:

3.14.1. Deve incluir, de forma unificada na console administrativa, área para monitoramento de experiência digital com medição de desempenho e a disponibilidade em tempo real de dispositivos, aplicativos e serviços, auxiliando na resolução de problemas e melhoria de produtividade;

3.14.2. Deve possuir, ao menos, os seguintes recursos de monitoramento:

3.14.2.1. Disponibilidade e desempenho de dispositivos em tempo real, indicando consumo de CPU, memória, disco, sinal WIFI, latência, jitter e perda de pacotes;

3.14.2.2. Análise da rota de comunicação de dados entre os dispositivos de usuários até o serviço contratado;

3.14.2.3. Mapa da infraestrutura de rede, fornecendo informações sobre a distribuição geográfica, conectividade e situação dos dispositivos;

3.14.2.4. Disponibilidade e desempenho do principal aplicativo de colaboração cadastrado, com opção para, pelo menos, Webex, Zoom e Microsoft Teams;

3.14.2.5. Desempenho e a disponibilidade de acesso aos aplicativos SaaS mais comuns, tais como AWS, Microsoft 365 e Google Suite.

3.15. Capacitação Técnica

3.15.1. O treinamento deverá ser completo para contemplar a instalação, customização, operação e administração da solução de SSE para 5 (cinco) funcionários da CONTRATANTE, na modalidade de Ensino a Distância (EAD), online e ao vivo;

3.15.2. O treinamento deverá ser ministrado para turma especifica para a CONTRATANTE;

3.15.3. Serão aceitos cursos oficiais do fabricante da solução.

3.16. Instalação e Configuração

3.16.1. O serviço de instalação e configuração deverá ser executado por técnico certificado pelo fabricante;

3.16.2. O serviço de instalação compreende as atividades de planejamento, instalação física, instalação lógica e finalização da solução no ambiente da CONTRATADA;

3.16.3. O serviço de configuração consiste em ajustar todos os parâmetros necessários (físicos e lógicos) para o funcionamento da solução e a sua adequação para funcionamento no ambiente da CONTRATADA atendendo aos requisitos dessa especificação.

3.17. Operação Assistida

3.17.1. A operação assistida deverá ocorrer durante 45 (quarenta e cinco) dias corridos a partir da instalação e configuração da solução na CONTRATANTE;

3.17.2. O serviço de operação assistida é composto por um conjunto

de atividades que permitem o treinamento e a capacitação da equipe da CONTRATANTE responsável pelas atividades de operação, manutenção preventiva e corretiva, transferindo todo o conhecimento e experiência necessária para a operação da solução;

3.17.3. Durante os 45 dias corridos, será prestado todo o suporte necessário para a operacionalidade da solução, minimizando o risco da implantação da solução e proporcionando as condições ideais para transferência da tecnologia envolvida em regime de treinamento enquanto trabalha, até que a CONTRATANTE possa assumir as atividades com sua própria equipe;

3.17.4. Durante a operação assistida também será necessário realizar, pela CONTRADADA, possíveis customizações e ajustes finais que forem identificados durante o período de instalação, configuração e operação assistida;

3.17.5. Por padrão, a prestação da operação assistida ocorrerá presencialmente nas dependências da CONTRATANTE ou remotamente a ser definido pela CONTRATANTE.

3.18. Suporte, Manutenção e Atualização de Versão

3.18.1. O suporte técnico compreende o diagnóstico e identificação de problemas, apoio técnico na utilização, correção de erros, defeitos (bugs) ou mau funcionamento sobre qualquer funcionalidade, recurso, componente ou módulo disponível de forma nativa efetuada pela CONTRATANTE;

3.18.2. O atendimento a um chamado de suporte deverá ocorrer por qualquer uma das seguintes formas: contato telefônico, envio de mensagem eletrônica (e-mail), acesso ao sítio (website) da CONTRATADA ou do fabricante da solução, com controle de acesso por senha;

3.18.3. A CONTRATANTE poderá efetuar um número ilimitado de chamados técnicos para a CONTRATADA, por qualquer uma das formas disponíveis, durante vigência do contrato vinculado a este Termo de Referência;

3.18.4. Caso acionado o suporte direto do fabricante, este deverá ter atendimento em português. Caso contrário, a CONTRATADA deverá ser responsável por intermediar os contatos entre o fabricante e a CONTRATANTE.

Documento assinado eletronicamente por **Heli Lopes Rios**, **Diretor(a) de Subsecretaria**, em 11/02/2025, às 14:28, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Arianne Caldeira do Carmo**, **Diretor(a) de Núcleo**, em 11/02/2025, às 14:30, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Daniel Santos Rodrigues**, **Diretor(a) de Secretaria**, em 11/02/2025, às 14:46, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Fernanda Marília Gonçalves Caetano**, **Assessor(a) I**, em 11/02/2025, às 15:13, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.trf6.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1110356** e o código CRC **38FCF626**.

PODER JUDICIÁRIO
TRIBUNAL REGIONAL FEDERAL DA 6ª REGIÃO
Subsecretaria de Planejamento Orçamentário

CLASSIFICAÇÃO DA DESPESA

Assunto: Classificação orçamentária para aquisição de solução de segurança de TIC com a finalidade de atender às necessidades de funcionamento dos sistemas do Tribunal Regional Federal da 6ª Região, por Sistema de Registro de Preços.

Informo que a classificação orçamentária mais adequada para a despesa é:

LOTES	ITENS	CATMAT / CATSER	OBJETO	UNIDADES REFERENCIAIS	QUANTIDADES	VALORES ESTIMADOS (R$)	NATUREZA DE DESPESA
01	01	484747	Appliances de Next Generation Firewall	Unidade	2	1.948.453,84	**449052-35** (Material de TIC - Permanente)
	02	27472	Licenciamentos para operações de Next Generation Firewall por 60 meses	Conjunto	1	2.172.763,87	**449040-05** (Aquisição de Software Pronto)
	03	26972	Instalação e Configuração	Conjunto	1	113.861,27	**339040-22** (Instalação de Equipamentos de TIC)
	04	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60	996.928,88	**339040-21** (Serviços Técnicos Profissionais de TIC)
	05	3840	Treinamento	Turma	1	106.394,95	**339040-20** (Treinamento/Capacitação em TIC)
02	06	27472	Web Application Firewall - Appliance Virtual	Unidade	1	1.179.426,29	**449040-05** (Aquisição de Software Pronto)
	07	26972	Instalação e Configuração	Conjunto	1	110.014,51	**339040-22** (Instalação de Equipamentos de TIC)
	08	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60	407.178,00	**339040-21** (Serviços Técnicos Profissionais de TIC)
	09	3840	Treinamento	Turma	1	22.635,63	**339040-20** (Treinamento/Capacitação em TIC)
03	10	27742	Serviço de Segurança de Borda (Security Service Edge - SSE)	Usuários	4.500	12.862.940,00	**339040-19** (Computação em Nuvem - Software como Serviço - SAAS)
	11	26972	Instalação e Configuração	Conjunto	1	93.600,00	**339040-22** (Instalação de Equipamentos de TIC)
	12	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60	1.867.380,00	**339040-21** (Serviços Técnicos Profissionais de TIC)
	13	3840	Treinamento	Turma	1	106.950,00	**339040-20** (Treinamento/Capacitação em TIC)

Ação Orçamentária:	**4257** - Julgamento de Causas na Justiça Federal
Plano Orçamentário:	**- TISI**: Capacitação de Servidores Efetivos e Comissionados das Unidades de Tecnologia da Informação e Segurança da Informação do Poder Judiciário (itens 05, 09 e 13); **- 0010**: Ações de Informática (demais itens).

À SELIT, para prosseguimento.

À SEORC, para ciência.

Atenciosamente,

Gláucia Maria Machado Rocha Ribeiro
Diretora da Subsecretaria de Planejamento Orçamentário - SUPLO/SECOF-TRF6

Documento assinado eletronicamente por **Glaucia Maria Machado Rocha Ribeiro**, **Diretor de Subsecretaria**, em 29/11/2024, às 19:34, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.trf6.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1031674** e o código CRC **2D4E3A66**.

PODER JUDICIÁRIO
TRIBUNAL REGIONAL FEDERAL DA 6ª REGIÃO
Subsecretaria de Infraestrutura

ESTUDO TÉCNICO PRELIMINAR - ETP (LEI 14.133/2021) 0990939

CONTRATAÇÃO DE SERVIÇOS E/OU AQUISIÇÃO DE BENS PERMANENTES E DE CONSUMO

Introdução

ETP foi elaborado conforme:

- a ordem dos elementos indicados no § 1º Art. 18 Lei 14.133/2021 (Nova Lei de Licitações e Contratos);

- o guia de suporte ao preenchimento de ETP 0366701, com orientações sobre conceitos, elaboração de textos e referências normativas.

Observação: conforme § 2º Art. 18 Lei 14.133/2021, ETP deverá conter ao menos os itens **I, IV, VI, VIII e XIII** e, quando não contemplar os demais, deverão ser incluídas as devidas justificativas.

I - Descrição da necessidade da contratação, considerado o problema a ser resolvido sob a perspectiva do interesse público

A atual infraestrutura de TIC que atende ao TRF6 foi preparada para o funcionamento de uma Seccional, razão pela qual o recebimento de sistemas anteriormente centralizados no TRF1 como o PJe, o SEI, Acordo 58, SIREA, eSiest, bancos de dados, entre outros, representou um consumo de recursos não previstos quando das aquisições, conforme cenário de escassez reportado por meio dos autos 0000724-85.2022.4.06.8000.

Diante do crescimento dos sistemas do TRF6, inúmeras aplicações anteriormente hospedadas no TRF1 passaram a ser publicadas na internet, o que representou o estabelecimento de um tráfego de conexões não dimensionado para a SJMG. Assim, a atual solução de segurança se mostrou insuficiente face à demanda cada vez maior de acessos, incluindo as vias automatizadas por robôs.

Destaca-se que as appliances de firewall Check Point 13500 alcançaram o chamado fim de utilização em junho de 2022 (vide relato do fabricante), o que obrigou a migração das operações para um modelo Open Server no ano de 2022, conforme Segundo Termo Aditivo ao Contrato n. 0035/2020 do TRF1 (Documento SEI TRF1 16656397).

Uma solução de segurança possui uma garantia recomendada de 04 anos com posterior substituição após a vigência, nos termos da Resolução CJF nº 477/2018, em razão da obsolescência técnica dos equipamentos. Por tal razão e considerando que os firewalls do TRF6 possuem mais de 8 anos de uso, além de não atenderem à atual demanda técnico-operacional, torna-se necessária a substituição dos equipamentos para adequação às necessidades de funcionamento do TRF6.

Outro ponto a se destacar é a dificuldade de tratamento dos acessos aos sistemas, em razão da indisponibilidade de WAF. Assim, os sistemas do TRF6 dependem de configurações individualizadas para o controle dos acessos automatizados frequentemente realizados por meio de robôs e bots, alguns dos quais de caracteres maliciosos.

Há, ainda, um elemento essencial à infraestrutura: a disponibilidade. Todos os sistemas do TRF6 devem estar disponíveis para funcionamento em regime de 24 x 7 (vinte e quatro horas, sete dias por semana), o que pode acarretar em situações de falhas em horários sem acompanhamento por equipe especializada e, consequentemente, em atraso para o início do atendimento. Considerando que os sistemas e serviços de TI do TRF6 sustentam a área finalística da instituição, torna-se cada vez mais importante que estejam hospedados em ambiente de infraestrutura tecnológica protegida e que garanta a disponibilidade e integridade das informações.

A contratação visa a adquirir uma solução de segurança de alta complexidade diante da necessidade de implantação aderente à LGDP, em substituição ao atual sistema obsoleto de proteção de perímetro de rede com a inclusão de novas funcionalidades de proteção de rede que compõem a plataforma de segurança de nova geração. A nova solução incluirá recursos de reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões, sistemas de detecção de invasão e sistemas de prevenção de intrusão, aplicações antimalware, inspeção de pacotes SSL/TLS, já que o tráfego é frequentemente criptografado para evitar a detecção e bloqueio de ameaças. Também permitirá o combate à falsificação de tráfego de acesso, o que dificulta a identificação e o bloqueio com base em assinaturas ou padrões específicos em razão do caráter aparentemente legítimo, ao parque tecnológico do TRF6.

Por tudo exposto, busca-se com a presente contratação:

a) Atualizar o parque tecnológico do TRF6;

b) Obter serviços de alta disponibilidade;

c) Aumentar a velocidade de operação entre os equipamentos;

d) Otimizar o desempenho da rede de dados;

e) Garantir a estabilidade operacional das comunicações do TRF6 e suas subseções judiciárias;

f) Aumentar a proteção de rede do TRF6, possibilitando a inspeção de tráfego com maior granularidade que a atualmente realizada;

g) Melhorar o desempenho e eficácia no controle de acesso ao perímetro de rede através de equipamentos com níveis de processamento e capacidade mais adequados;

h) Aumentar a disponibilidade das aplicações, evitando o comprometimento da capacidade do firewall em eventuais situações de ataque;

i) Possuir viabilidade para realizar futuras expansões da capacidade e granularidade da rede do Tribunal;

j) Possibilitar a ampliação da segmentação da rede com o objetivo de reduzir os riscos de segurança;

k) Aumento da resiliência em caso de ataques;

l) Diminuir o tempo de análise e resolução de problemas.

II - Demonstração da previsão da contratação no plano de contratações anual, sempre que elaborado, de modo a indicar o seu alinhamento com o planejamento da Administração

- Resolução CNJ nº 370, de 28 de janeiro de 2021 - Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);
- Resolução CJF nº 685, de 15 de dezembro de 2020 - Plano Estratégico de Tecnologia da Informação da Justiça Federal;
- Portaria PRESI 125/2023 - Plano Estratégico Regional da Justiça Federal da 6ª Região para o ciclo 2023-2026.

Macrodesafio: Fortalecimento da Estratégia Nacional de TIC e de Proteção de Dados

Objetivos Estratégicos da Justiça Federal:

1) Aperfeiçoar e assegurar a efetividade dos serviços de TI para a Justiça Federal

Indicadores	Metas
1 - Índice de satisfação dos clientes internos com os serviços de TI.	1 - Atingir, até 2025, 85% de satisfação dos clientes internos de TI.
2 - Índice de satisfação dos clientes externos com os serviços de TI.	2 - Atingir, até 2026, 80% de satisfação dos clientes externos de TI.

III - Requisitos da contratação

Definição dos requisitos (Art. 18, § 1º, III, da Lei n. 14.133/2021)

1. Requisitos de Negócio

   1.1. Assegurar a efetividade dos serviços de TI para o TRF6, através da continuidade dos serviços de segurança de dados e aplicações e de proteção contra ameaças;

   1.2. Assegurar a proteção dos dados dos sistemas e dos usuários do TRF6 de acordo com a Política de Segurança da Informação do CJF, aplicável em razão da falta de norma própria.

2. Requisitos de Garantia

   2.1. A garantia da solução deve permitir reparar eventuais falhas e substituir peças com defeito por outras de configuração idêntica ou superior;

   2.2. A garantia da solução deve permitir a atualização dos produtos licenciados assim que novas versões e releases dos softwares que fizerem parte da solução contratada estiverem disponíveis.

3. Requisitos Técnicos

   3.1. Os serviços de suporte deverão ser capazes de atender às demandas de compatibilidade da solução de segurança com a infraestrutura computacional existente no TRF6.

   3.2. As especificações dos itens

4. Requisitos de Suporte

   4.1. Será prestado serviço de suporte técnico durante toda a vigência do contrato, com direito a atualizações de versões da solução que incorporem correções de defeitos e melhorias implementadas pelos fabricantes.

5. Requisitos de Manutenção

   5.1. A solução proposta deverá possuir garantia do fabricante de 05 anos para entrega de peças on-site;

   5.2. Atendimento 24x7 nas dependências do TRF6;

   5.3. Substituir componentes e peças defeituosos ou com falhas, trocas periódicas das peças internas, discos e demais componentes que apresentarem problemas técnicos durante a vigência do contrato, utilizando de produtos originais, novos e de primeiro uso, garantidos pelo fabricante;

5.4. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos no processo de contratação, com observância às recomendações aceitas pela boa técnica, normas e legislação, bem como observar conduta adequada na utilização dos materiais, equipamentos, ferramentas e utensílios;

5.5. Possibilitar o suporte técnico e especializado, remoto ou presencial, entre o CONTRATANTE e o fabricante sem novos ônus ou custos contratuais;

5.6. Executar todas as atividades de instalação, atualização, configuração e migração de acordo com o planejamento aprovado pela área técnica;

5.7. Realizar manutenção corretiva, que compreende providências para reparar e corrigir os componentes da solução contratada em seu pleno estado de funcionamento, removendo definitivamente os defeitos eventualmente apresentados;

5.8. Garantir o funcionamento do ambiente com relação à solução instalada pela CONTRATADA, incluindo todos os serviços necessários para manutenção da disponibilidade da solução, inclusive de configurações e fornecimento de "firmwares", "fixes" e "releases", durante toda a vigência do contrato;

5.9. Os serviços serão solicitados mediante a abertura de um chamado efetuado por técnicos da contratante, via chamada telefônica local, a cobrar ou 0800, e-mail, website ou chat do fabricante ou à empresa autorizada (em português – para o horário comercial – horário oficial de Brasília) e constatada a necessidade, o fornecedor deverá providenciar o deslocamento do equipamento, bem como seu retorno ao local de origem sem qualquer ônus ao contratante.

6. Requisitos de Instalação

6.1. A realização dos serviços deve ser planejada de acordo com disponibilidade de ambas as partes. O planejamento anterior ao serviço deverá ser realizado de forma on-site nas dependências da CONTRATANTE;

6.2. O planejamento dos serviços de instalação deve resultar num documento tipo SOW (em tradução livre, escopo de trabalho). Neste documento devem conter a relação, descrição e quantidades dos produtos fornecidos, descrição da infraestrutura atual e desejada, detalhamento dos serviços que serão executados, premissas do projeto, locais e horários de execução dos serviços, condições de execução dos serviços, pontos de contato da CONTRATADA e CONTRATANTE, cronograma de execução do projeto em etapas, com responsáveis e data e início e fim (se aplicável), relação da documentação a ser entregue ao final da execução dos serviços, responsabilidade da CONTRATADA, plano de gerenciamento de mudanças, itens excluídos no projeto e termo de aceite. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes;

6.3. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, devendo a CONTRATADA sugerir as configurações de acordo com normas técnicas e boas práticas, cabendo à CONTRATANTE a sua aceitação expressa ou recusa nos casos de não atendimento das condições estabelecidas;

6.4. Após a instalação, a solução deverá ser monitorada on-site nas dependências da CONTRATANTE pelo prazo mínimo de 8 (oito) horas corridas, observando as condições de funcionamento e performance dos equipamentos, sendo possível o troubleshooting em caso de problemas ou não conformidades na operação;

6.5. Ao final da instalação, deverá ser realizado o repasse de configurações hands-on, de forma on-site nas dependências da CONTRATANTE apresentando as configurações realizadas. A CONTRATANTE disponibilizará o local adequado para a transferência do conhecimento e acesso a solução em produção;

6.6. Os serviços deverão ser realizados por pessoal técnico experiente e certificado pelo fabricante da solução. Em momento anterior à instalação, a CONTRATANTE poderá solicitar os comprovantes da qualificação profissional do(s) técnico(s) que executará(ão) os serviços, sendo direito da mesma a sua aceitação ou exigência de troca de profissional no caso de este não satisfazer às condições supramencionadas;

6.7. Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados no projeto (relatório as-built), etapas de execução e toda informação pertinente para posterior continuidade e manutenção da solução instalada, como usuários e endereços de acesso, configurações realizadas e o resumo das configurações dos equipamentos. Este relatório deve ser enviado com todas as informações em até 15 dias após a finalização dos serviços;

6.8. Nos valores cotados devem estar inclusas todas as despesas com deslocamento, alimentação e estadia para realização dos serviços (onsite) nos locais de presença da CONTRATANTE. Os funcionários da CONTRATADA deverão possuir todo o ferramental necessário ao exercício das suas atividades;

6.9. A CONTRATADA deverá garantir a confidencialidade das informações, dados e senhas compartilhadas da CONTRATANTE;

6.10. A execução dos serviços ocorrerá na sede da CONTRATANTE;

6.11. Durante as atividades realizadas na prestação do serviço, o técnico da CONTRATADA deverá demonstrar à equipe técnica de acompanhamento da CONTRATANTE como instalar e configurar os equipamentos e os softwares fornecidos (instalação assistida);

6.12. As atividades deverão ser realizadas dentro do horário comercial.

7. Requisitos de Conformidade

7.1. Deverá fazer parte do catálogo de produtos comercializados pelo fabricante e não ter sido descontinuado;

7.2. Deverá ser novo, sem uso, e constar no site do fabricante (documento oficial e público) como em linha de produção;

7.3. Deverá permitir a utilização de todas as funcionalidades, tecnologias e recursos especificados, durante a vigência CONTRATADA, irrestrita e sem necessidade de licenciamentos ou ônus adicionais.

8. Requisitos Temporais

8.1. Apresentar plano de implantação contendo os requisitos de instalação e cronograma de entrega, instalação, configuração e disponibilização da solução, em até 30 (trinta) dias corridos da assinatura do contrato;

8.2. Entregar os produtos no prazo máximo de até 90 (noventa) dias corridos, a contar da assinatura do contrato;

8.3. A entrega deverá ser formalizada mediante comunicação escrita da CONTRATADA ao CONTRATANTE;

8.4. Executar a conferência dos produtos especificados, conjuntamente com representantes da CONTRATADA, para emissão do Termo de Recebimento Provisório;

8.5. Antes de findar o prazo fixado a empresa CONTRATADA poderá formalizar, de forma devidamente fundamentada, pedido de sua prorrogação, cujas razões expostas serão examinadas pela administração do CONTRATANTE, que decidirá pela prorrogação do prazo ou aplicação das penalidades previstas;

8.6. A CONTRATADA receberá cópia do "Termo de Recebimento Provisório" após a entrega e conferência dos produtos em até 5 (cinco) dias úteis da confirmação de entrega, contados do primeiro dia imediatamente posterior à confirmação de entrega dos itens no CONTRATANTE, desde que não haja pendências de responsabilidade da CONTRATADA;

8.7. Concluir, no prazo de 30 (trinta) dias corridos, a contar da emissão do termo de recebimento provisório, a implantação e configuração dos produtos, em plena compatibilidade com o ambiente computacional do CONTRATANTE e em conformidade com a proposta técnica apresentada, cumprindo ainda todas as demais cláusulas de garantia e atendimento técnico constantes do contrato, nos prazos e termos ali estipulados;

8.8. A CONTRATADA receberá cópia do "Termo de Recebimento Definitivo", que deverá ser providenciado pelo CONTRATANTE no prazo máximo de 10 (dez) dias úteis, após manifestação da CONTRATADA de conclusão dos serviços e comprovação de atendimento de todas as fases, desde que a CONTRATADA atenda a todas as solicitações e que não haja pendências de sua responsabilidade;

8.9. Os serviços de suporte e garantia deverão estar disponíveis para atendimento durante os 07 (sete) dias corridos da semana, 24 (vinte e quatro) horas por dia;

8.10. Considerar o horário das 07 horas às 20 horas como de horário normal de expediente, para os dias úteis.

9. Requisitos de Sustentabilidade Ambiental

9.1. A CONTRATADA será responsabilizada por qualquer prejuízo que venha causar ao TRF6 por ter suas atividades suspensas, paralisadas ou proibidas por falta de cumprimento de normas ligadas ao software e ainda aos serviços elencados no presente Termo de Referência;

9.2. A CONTRATADA deverá comprovar que os produtos ofertados atendem aos critérios de segurança, compatibilidade eletromagnética e eficiência energética, previstos no art. 3º, inciso II, do Decreto n. 7.174, de 12 de maio de 2010, regulamentado pela Portaria INMETRO n. 170, de 10 de abril de 2012;

9.3. Só será admitida a oferta de bens de informática e/ou automação que não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr (VI)), cádmio (Cd), bifenil polibromados (PBBs), éteres difenil-polibromados (PBDEs), conforme o art. 5º, inciso IV, da IN MPOG 01, de 19 de janeiro de 2010;

9.4. As comprovações dos dois itens anteriores, quando exigidas pela CONTRATANTE, poderá ser feita mediante apresentação de certificação emitida por instituição pública oficial ou instituição credenciada, ou por qualquer outro meio de prova, em especial laudo pericial, que ateste que os bens fornecidos cumprem com as exigências do edital, conforme art. 42, inciso III, da Lei 14.133, de 1º de abril de 2021;

9.5. A CONTRATADA deverá, para a execução do contrato, fornecer aos empregados os equipamentos de segurança que se fizerem necessários, para a execução de serviços, conforme disposto no art. 6°, inciso IV, da Instrução Normativa SLTI/MPOG n. 01, de 19 de janeiro de 2010;

9.6. A CONTRATADA deverá se atentar às normas em vigor atinentes à sustentabilidade expressas na 2ª edição do Manual de Sustentabilidade de compras e contratos do Conselho da Justiça Federal, instituído pela Portaria CJF n. 96, de 10 de fevereiro de 2023;

9.7. A CONTRATADA deverá respeitar a legislação vigente e as normas técnicas, elaboradas pela ABNT e pelo INMETRO para aferição e garantia de aplicação dos requisitos mínimos de qualidade e acessibilidade do software e ainda dos serviços elencados no Termo de Referência.

10. Requisitos Legais e Normativos Aplicáveis ao Objeto da Contratação

10.1. Política de Segurança da Informação do CJF - Resolução CJF 006/2008;

10.2. Lei n. 14.133, de 1º de abril de 2021;

10.3. Resolução CNJ 468, de 15 de julho de 2022.

IV - Estimativas das quantidades para a contratação, acompanhadas das memórias de cálculo e dos documentos que lhes dão suporte, que considerem interdependências com outras contratações, de modo a possibilitar economia de escala

A pesquisa de preços estimados para a elaboração do DOD 0751599, realizada a partir de preços públicos, levantou os valores abaixo detalhados:

- Cenário 1 (equipamentos e licenciamentos):

Itens	Descrições	Valores Médios Anuais (R$)	Valores Médios 05 Anos (R$)
01	Solução em alta disponibilidade (appliance) FW	1.670.693.66	1.670.693,66
02	Licenciamentos Anuais FW	711.731,09	3.558.655,44
03	Solução em alta disponibilidade (appliance) WAF Controle	1.017.675,35	1.017.675.35

04	Licenciamentos Anuais WAF Controle	966.182,54	4.830.912,69
05	Solução em alta disponibilidade (appliance) WAF Balanceador	1.694.999,94	1.694.999,94
06	Licenciamentos Anuais WAF Balanceador	934.053,38	4.670.266,92
09	Instalação	99.409,07	99.409,07
10	Suporte	223.907,57	1.119.537,85
11	Treinamento	66.766,30	67.766,30
TOTAIS (R$) **		**7.385.418,89**	**18.728.917,21**

- Cenário 2 (equipamentos, licenciamentos e serviços continuados):

Itens	Descrições	Valores Médios Anuais (R$)	Valores Médios 05 Anos (R$)
01	Solução em alta disponibilidade (appliance) FW	1.670.693.66	1.670.693,66
02	Licenciamentos Anuais FW	711.731,09	3.558.655,40
07	SaaS Proteção (serviço continuado)	1.126.870,44	5.634.352,20
08	Franquia Adicional	897.750,00	4.488.750,00
09	Instalação	99.409,07	99.409,07
10	Suporte	223.907,57	1.119.537,85
11	Treinamento	66.766,30	66.766,30
TOTAIS (R$) **		**4.797.128,13**	**16.638.164,52**

** Valores estimados com base em contratações públicas similares, portanto ainda sem a adequação conforme as volumetrias do TRF6.

Atualmente, a solução de segurança de dados do TRF6 é composta pelo seguinte cenário:

1. Contrato nº 0035/2020 - TRF1 (3º termo aditivo - SEI TRF1 - 19188174)

1.1. Licenciamento Open Server Check Point R81.20 Jumbo:

1.1.1. Vigência até 05/11/2024;

1.1.2. Incluído suporte sob demanda às operações;

1.1.2. Valor anual: R$ 423.769,50.

2. Contrato nº 016/2023 (0298363):

2.1. Licenciamento de Antivírus ESET Protect Enterprise:

2.1.1. Vigência até 25/09/2028;

2.1.2. Incluído suporte sob demanda às operações;

2.1.2. Valor anual (suporte): R$ 6.000,00.

Considerando que a atual solução de segurança é precária, obsoleta e que não atende às necessidades de segurança e proteção de dados e aplicações do TRF6, torna-se necessária a aquisição de uma nova solução de segurança de dados que ofereça um melhor serviço de continuidade e integridade das operações e que minimize as exposições contra ameaças.

V - Levantamento de mercado, que consiste na análise das alternativas possíveis, e justificativa técnica e econômica da escolha do tipo de solução a contratar

Com base em opções disponíveis no mercado, foram levantadas as diferentes soluções de TIC que podem atender às necessidades do TRF6:

5.1. Solução nº 1 - Utilização de Softwares Livres

5.1.1. No universo de softwares livres, existem diversas soluções. Ocorre que todo uso de software livre demanda esforços técnicos de desenvolvimento e customização da solução.

5.1.2. Cumpre registrar que o quadro de servidores da SECTI é reduzido e a demanda de serviços gerada pelos sistemas do TRF6 sobrecarregou, sobremaneira, os trabalhos desta Diretoria, sem, contudo, completar o quadro funcional que já vinha defasado de mão de obra especializada.

5.1.3. É inegável que uma prestação de serviços eficiente está condicionada à existência de um contingente de pessoal capacitado e em número suficiente para atender à demanda de usuários dos nossos serviços, pois a insuficiência de pessoal além de contribuir para que o serviço prestado seja ineficiente e moroso, faz com que haja acúmulo e sobrecarga de trabalho nos poucos servidores existentes. Apesar de ser cediço que tal situação não é adequada, deve-se reforçar que os servidores da Secretaria de Tecnologia da Informação cumprem sua missão institucional com inegável zelo e esforço, pois, uma vez que não há possibilidade de desligamento dos sistemas informatizados que operam, a equipe tem trabalhado no decorrer dos sete dias da semana.

5.1.4. Pelo exposto e considerando que o TRF6 não conta com profissionais especializados e em quantidades necessárias para a operacionalização das atividades de desenvolvimento e customização dos softwares livres, a alternativa não atende à necessidade.

5.2. Solução nº 2 - Utilizar a atual solução de segurança

5.2.1. Não é possível seguir com a atual solução de segurança, uma vez que depende de licenciamento vinculado a contrato do TRF1 e já não atende à demanda necessária;

5.2.2. A solução de Next Generation Firewall atual foi virtualizada em razão da descontinuidade do modelo de appliance Check Point 13500 em junho de 2022, conforme informações do fabricante disponíveis no link (acesso em 25/09/2024);

5.2.3. A atual solução não possui tratamento de aplicações e balanceamento de carga, o que impede a utilização dinâmica das conexões de internet;

5.2.4. Não há disponibilidade, ainda, de solução de gerenciamento de acessos, o que impede o controle rigoroso das operações realizadas pelos usuários do TRF6 e Subseções Judiciárias.

5.3. Solução nº 3 - Adquirir nova solução de segurança

5.3.1. De forma a viabilizar o atendimento às necessidades e de acordo com as tecnologias disponíveis no mercado, a nova solução de segurança deve incluir os itens abaixo relacionados:

5.3.1.1. Solução de alta disponibilidade de Next Generation Firewall - NGFW, incluindo os respectivos licenciamentos e os serviços de instalação, configuração, suporte técnico e treinamento;

5.3.1.2. Solução de alta disponibilidade de Web Application Firewall - Appliance Virtual, incluindo os respectivos licenciamentos e os serviços de instalação, configuração, suporte técnico e treinamento;

5.3.1.3. Solução de Serviço de Segurança de Borda (*Security Service Edge* - SSE), incluindo os respectivos licenciamentos e os serviços de instalação, configuração, suporte técnico e treinamento.

5.3.2. A equipe de planejamento realizou um comparativo entre os principais requisitos com base em dados disponibilizados no site de cada fabricante e por meio dos diversos apontamentos realizados pelos parceiros dos principais líderes de mercado.

5.3.2.1. A análise de contratações públicas similares permitiu identificar os modelos de produtos e serviços incompatíveis com as necessidades do TRF6, conforme detalhamento abaixo:

OBJETO	ÓRGÃO	FONTES	JUSTIFICATIVAS
SaaS Proteção	TRF3	0751373 0751375	Serviço não realiza a inspeção do tráfego MTLS e o balanceamento das aplicações.
WAF Appliance	TRE-PI	0751378	Solução a ser adquirida em coparticipação em contratação conduzida pelo CJF, nos termos dos autos SEI 0010176-51.2024.4.06.8000.
WAF Appliance	Banco do Nordeste	0751429	Solução a ser adquirida em coparticipação em contratação conduzida pelo CJF, nos termos dos autos SEI 0010176-51.2024.4.06.8000.
WAF Appliance	TCE-MT	0751463	Solução a ser adquirida em coparticipação em contratação conduzida pelo CJF, nos termos dos autos SEI 0010176-51.2024.4.06.8000.
WAF Appliance	STJ	0751506	Solução a ser adquirida em coparticipação em contratação conduzida pelo CJF, nos termos dos autos SEI 0010176-51.2024.4.06.8000.
NGFW	UFF	0751530	Solução inferior tecnicamente às necessidades.
WAF Appliance	CAPES	0751540	Solução a ser adquirida em coparticipação em contratação conduzida pelo CJF, nos termos dos autos SEI 0010176-51.2024.4.06.8000.
SaaS Proteção	TCE-RR	0751548	Serviço não realiza a inspeção do tráfego MTLS e o balanceamento das aplicações.
WAF Appliance Virtual	CIPP - Gov-CE	0751562	Solução inferior tecnicamente às necessidades.
ZTNA	UDESC	0837652	Solução inferior tecnicamente às necessidades.
ZTNA	MAP	0837723	Solução inferior tecnicamente às necessidades.

5.4. Análise e comparação entre as soluções de TIC avaliadas:

Requisito	ID da Solução	Sim	Não	Não se Aplica
A Solução encontra-se implantada outro órgão ou entidade Administração Pública Federal?	Solução 1	X		
	Solução 2			
	Solução 3			
A Solução encontra-se implantada em outro órgão ou entidade da Justiça Federal?	Solução 1		X	
	Solução 2	X		
	Solução 3		X	
A Solução está disponível no Portal do Software Público Brasileiro?	Solução 1		X	
	Solução 2			
	Solução 3			
A Solução é um software livre ou software público?	Solução 1	X		
	Solução 2		X	
	Solução 3		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	Solução 1			X
	Solução 2			
	Solução 3			
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			
	Solução 3			
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Judiciário – MoReq-Jus?	Solução 1			X
	Solução 2			
	Solução 3			

5.5. Justificativa da solução de TIC escolhida, considerando o ciclo de vida do objeto.

5.5.1. A solução que melhor atende às necessidades do TRF6 é a solução nº 03, pelos seguintes fundamentos:

5.5.1.1. A solução de segurança proposta se encontra de acordo com as recomendações do Manual de Referência de Segurança Cibernética do CNJ, pois inclui os mecanismos de perímetro necessários à restrição dos acessos não autorizados;

5.5.1.2. Permite a operação em alta disponibilidade;

5.5.1.3. Representa um relevante incremento da velocidade de operação entre os equipamentos e sistemas;

5.5.1.4. Otimiza o desempenho das aplicações;

5.5.1.5. Incrementa a proteção de rede do TRF6, possibilitando a inspeção de tráfego com maior granularidade que a atual;

5.5.1.6. Permite o controle de acesso ao perímetro de rede através de equipamentos com níveis de processamento e capacidade mais adequados;

5.5.1.7. Aumenta a disponibilidade das aplicações, evitando o comprometimento da capacidade do firewall em eventuais situações de ataque;

5.5.1.8. Viabiliza futuras expansões da capacidade e granularidade da rede do Tribunal;

5.5.1.9. Possibilita a ampliação da segmentação da rede com o objetivo de reduzir os riscos de segurança;

5.5.1.10. Aumenta consideravelmente a resiliência em caso de ataques;

5.5.1.11. Diminui consideravelmente o tempo de análise e resolução de problemas.

5.5.2. O ambiente do TRF6 atual conta apenas com uma solução de firewall com licenciamento renovado anualmente e em operação em modelo *Open Server*, em virtude do encerramento das operações das appliances Check Point 13500.

5.5.2.1. A equipe técnica conta com apoio de suporte mantido por contrato celebrado pelo TRF1 e recentemente assumido pelo TRF6, cuja renovação será realizada para garantir o funcionamento da solução até que a presente contratação seja concluída;

5.5.2.2. A falta da solução de WAF impede o controle e balanceamento das aplicações, o que demanda a necessidade de bloqueio dos acessos ilegítimos de forma manual e direta nos *proxies*;

5.5.2.3. A falta de uma solução de SSE obriga a utilização de solução de acesso *open source* VPN sem quaisquer controles sobre as máquinas de origem das conexões, o que representa uma grande exposição aos riscos de segurança para a rede interna e aplicações do TRF6.

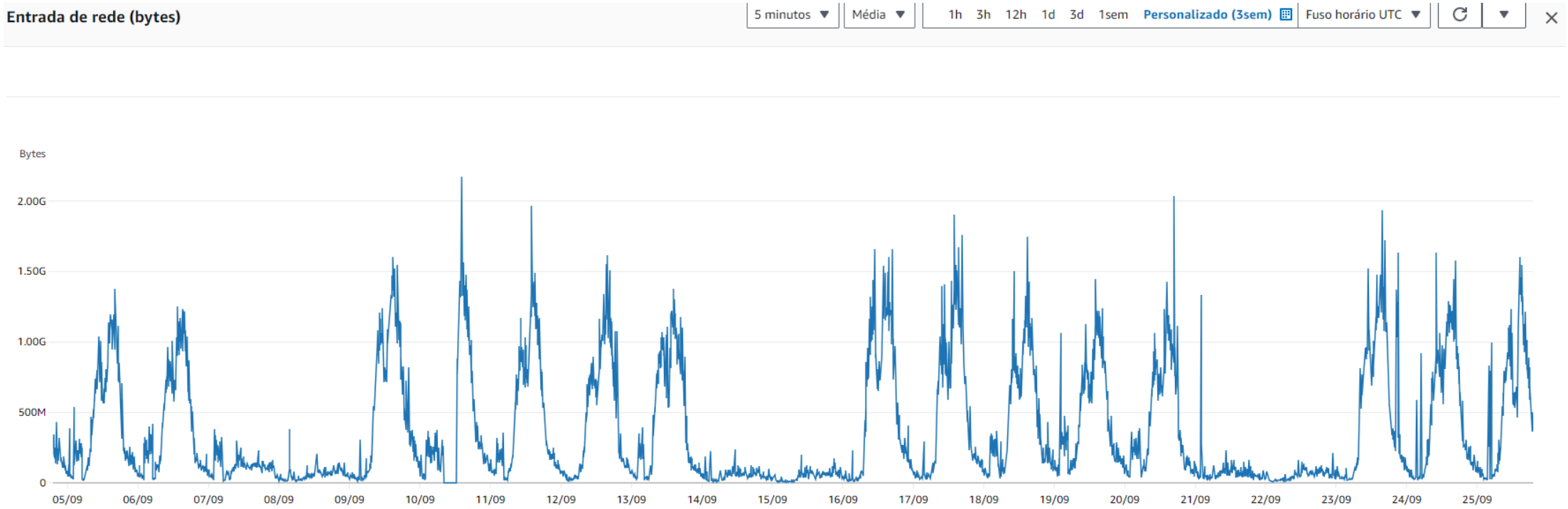
5.5.3. A previsão de contratação de soluções de WAF providas por meio de appliance virtual possibilita ao TRF6 a operação híbrida, pois o licenciamento é aplicável aos ambientes *on premises* e de nuvem.

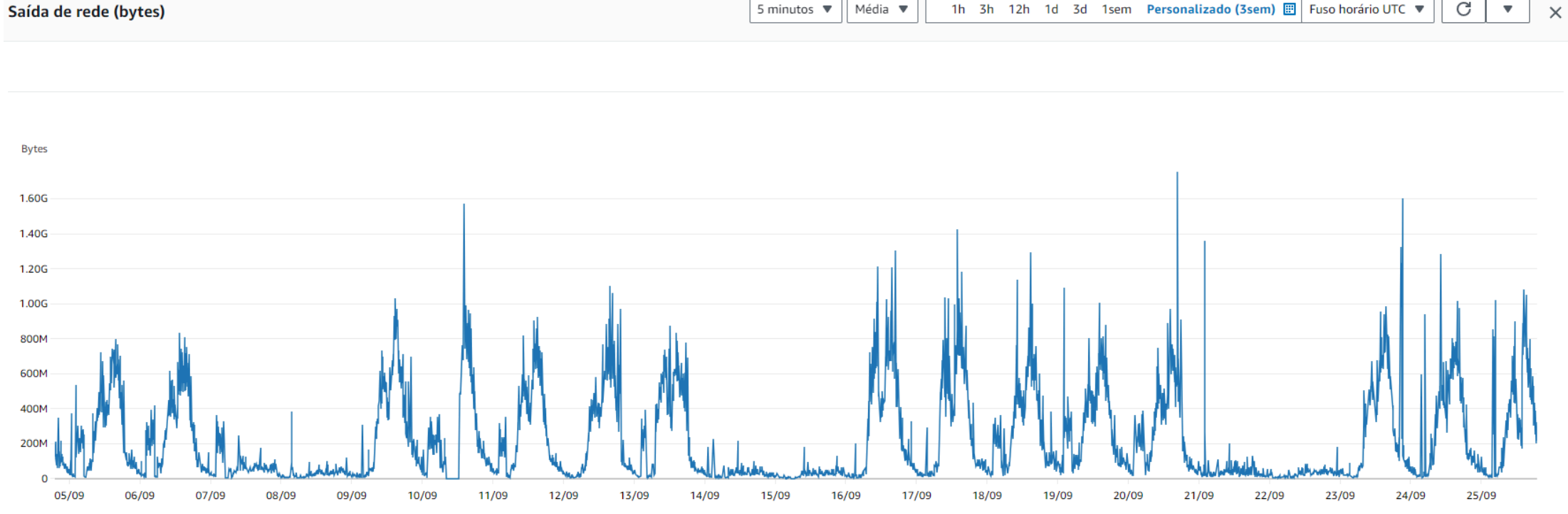
5.5.3.1. Em razão da coparticipação em contratação conduzida pelo CJF (0788920), a aquisição da solução de WAF e respectivos licenciamentos foi desmembrada da presente contratação e seguirá por meio dos autos SEI 0010176-51.2024.4.06.8000.

5.5.4. A presente aquisição de solução de segurança incluiu as ferramentas de Serviço de Segurança de Borda (*Security Service Edge* - SSE), em razão da necessidade de controle dos acessos externos dos usuários.

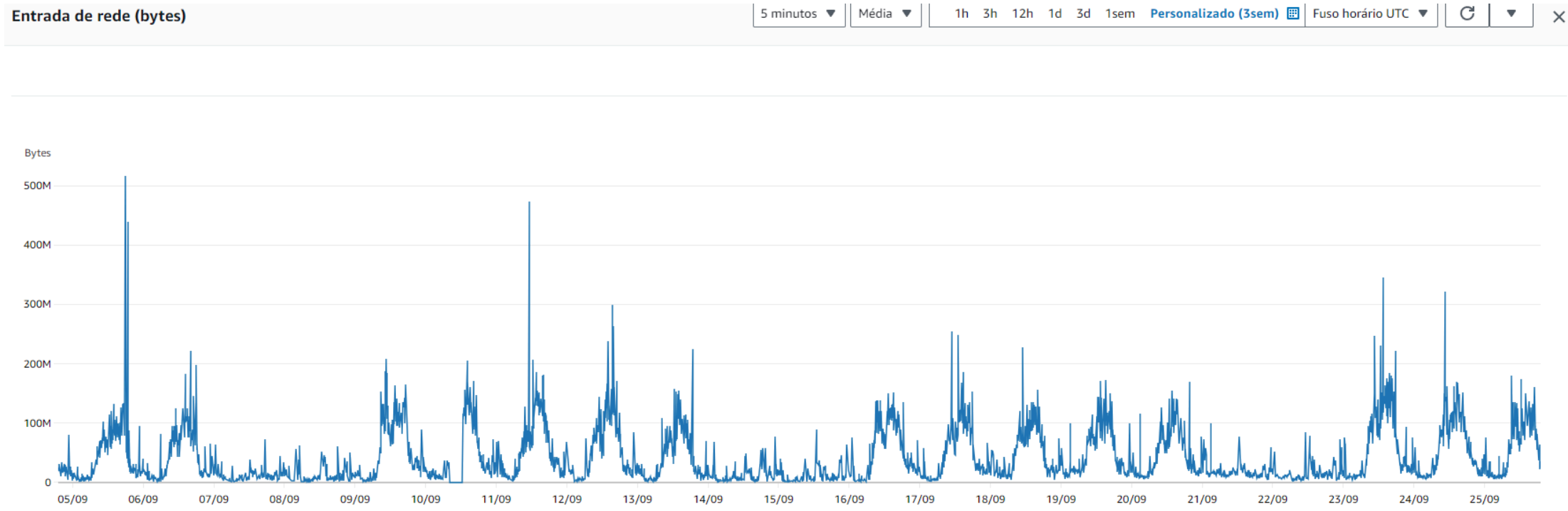
5.5.5. O dimensionamento das soluções foi realizado com base nos indicadores de tráfego e número de acessos simultâneos e totais dos serviços mais relevantes do TRF6, conforme detalhamento abaixo:

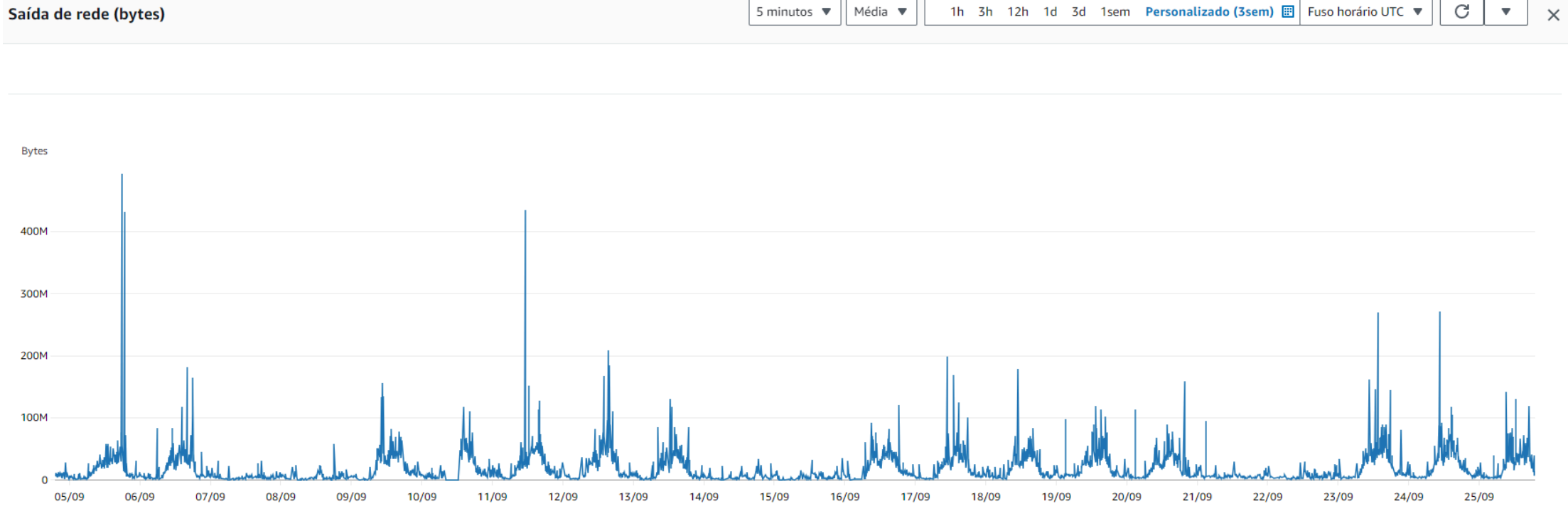
eproc 1G



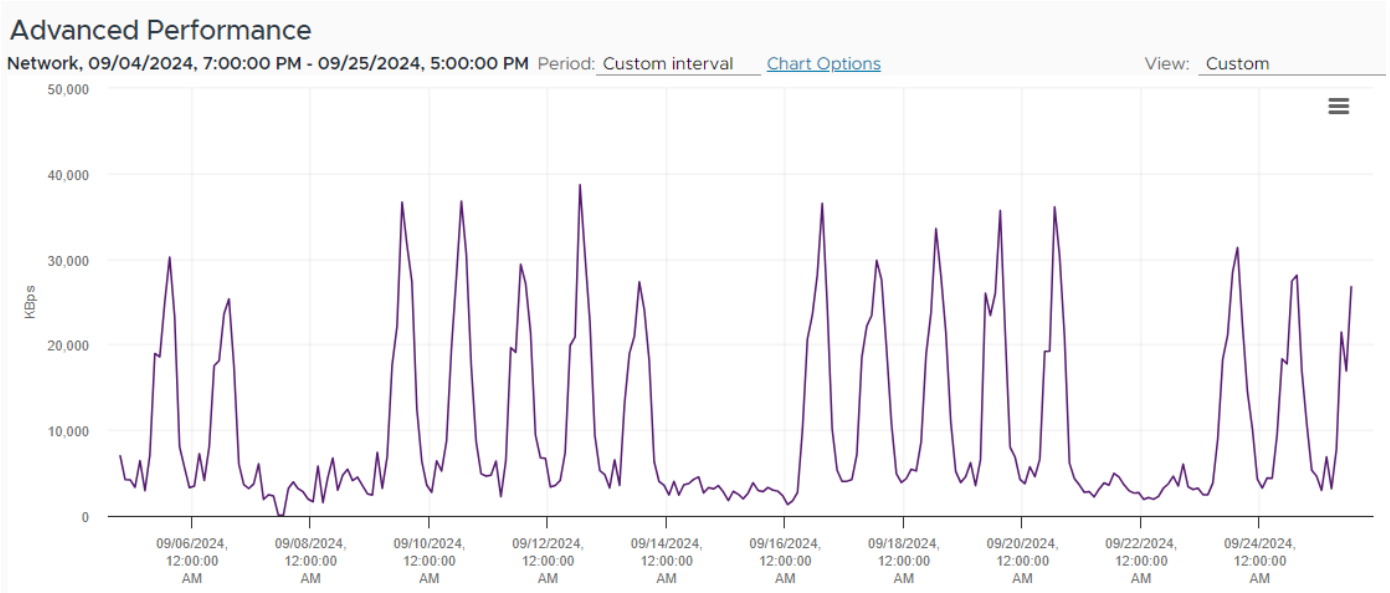

Saída de rede (bytes)
5 minutos
Média
1h 3h 12h 1d 3d 1sem Personalizado (3sem)
Fuso horário UTC
Bytes
1.60G
1.40G
1.20G
1.00G
800M
600M
400M
200M
0
05/09 06/09 07/09 08/09 09/09 10/09 11/09 12/09 13/09 14/09 15/09 16/09 17/09 18/09 19/09 20/09 21/09 22/09 23/09 24/09 25/09

eproc 2G

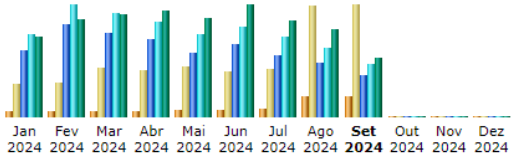

Entrada de rede (bytes)
5 minutos
Média
1h 3h 12h 1d 3d 1sem Personalizado (3sem)
Fuso horário UTC
Bytes
500M
400M
300M
200M
100M
0
05/09 06/09 07/09 08/09 09/09 10/09 11/09 12/09 13/09 14/09 15/09 16/09 17/09 18/09 19/09 20/09 21/09 22/09 23/09 24/09 25/09


Saída de rede (bytes)
5 minutos
Média
1h 3h 12h 1d 3d 1sem Personalizado (3sem)
Fuso horário UTC
Bytes
400M
300M
200M
100M
0
05/09 06/09 07/09 08/09 09/09 10/09 11/09 12/09 13/09 14/09 15/09 16/09 17/09 18/09 19/09 20/09 21/09 22/09 23/09 24/09 25/09

PJe 1G

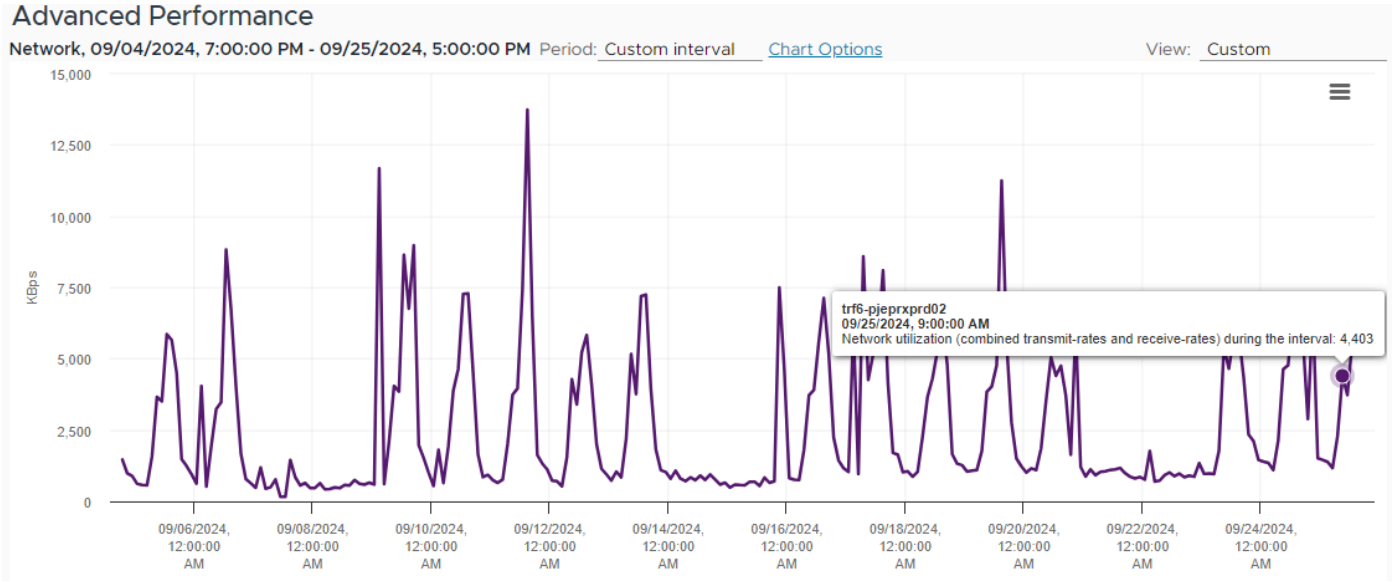

Advanced Performance
Network, 09/04/2024, 7:00:00 PM - 09/25/2024, 5:00:00 PM
Period: Custom interval
Chart Options
View: Custom
50,000
40,000
30,000
20,000
10,000
0
KBps
09/06/2024, 12:00:00 AM
09/08/2024, 12:00:00 AM
09/10/2024, 12:00:00 AM
09/12/2024, 12:00:00 AM
09/14/2024, 12:00:00 AM
09/16/2024, 12:00:00 AM
09/18/2024, 12:00:00 AM
09/20/2024, 12:00:00 AM
09/22/2024, 12:00:00 AM
09/24/2024, 12:00:00 AM

Histórico mensal

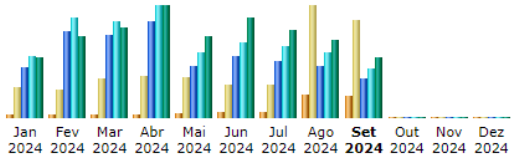


Mês	Visitantes únicos	Numero de visitas	Páginas	Hits	Bytes
Jan 2024	282,466	1,617,684	159,989,768	200,825,443	6.51 TB
Fev 2024	279,897	1,638,735	223,614,352	271,312,800	7.92 TB
Mar 2024	294,381	2,350,614	203,892,307	253,165,670	8.25 TB
Abr 2024	266,606	2,250,684	188,101,855	232,040,636	8.56 TB
Mai 2024	329,933	2,430,559	155,817,547	200,325,618	7.96 TB
Jun 2024	358,789	2,221,693	175,565,838	217,659,521	9.04 TB
Jul 2024	378,018	2,340,047	149,718,132	193,599,365	7.75 TB
Ago 2024	1,013,989	5,420,881	130,438,491	168,337,215	7.05 TB
Set 2024	1,007,870	5,423,532	100,601,439	129,208,210	4.79 TB
Out 2024	0	0	0	0	0
Nov 2024	0	0	0	0	0
Dez 2024	0	0	0	0	0
Total	4,211,949	25,694,429	1,487,739,729	1,866,474,478	67.83 TB

PJe 2G

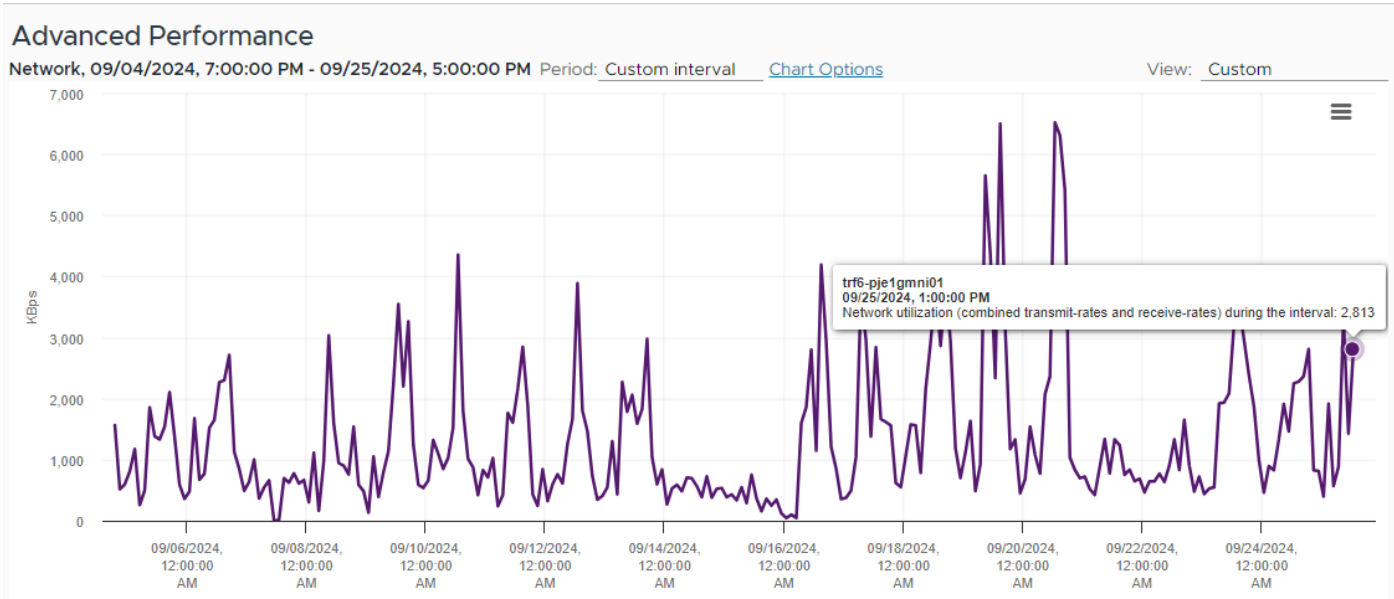


Histórico mensal



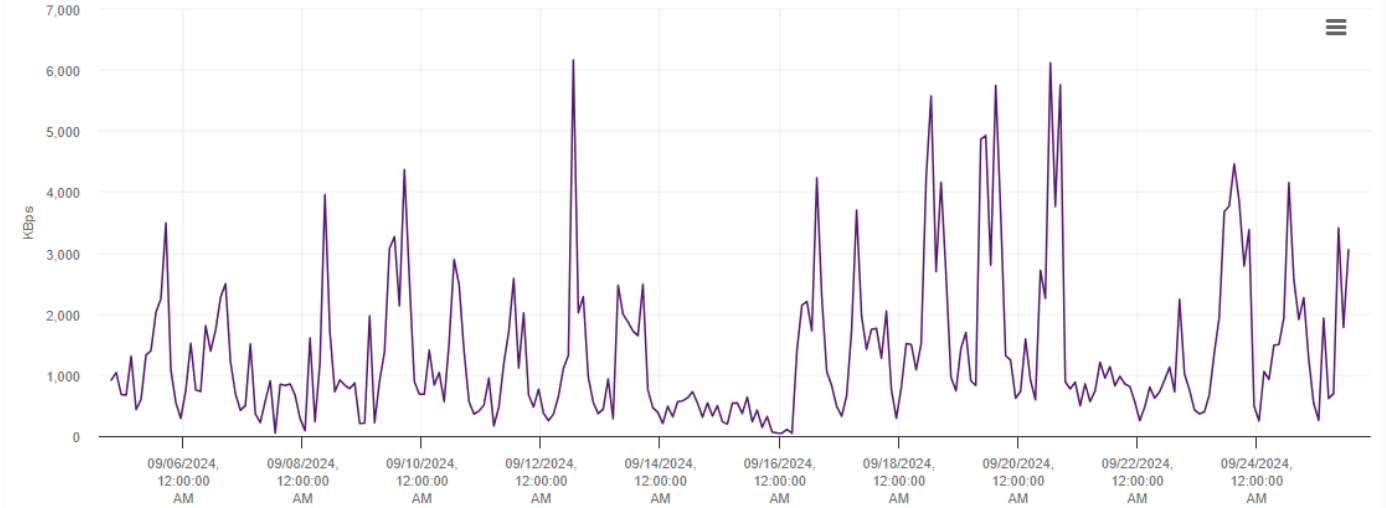
Mês	Visitantes únicos	Numero de visitas	Páginas	Hits	Bytes
Jan 2024	121,534	1,140,055	50,603,369	62,085,542	1.15 TB
Fev 2024	119,268	1,039,973	86,411,059	99,672,273	1.56 TB
Mar 2024	132,773	1,495,079	82,236,181	96,588,211	1.72 TB
Abr 2024	137,114	1,580,865	96,189,063	112,085,767	2.14 TB
Mai 2024	185,189	1,532,332	51,570,086	65,929,383	1.55 TB
Jun 2024	214,194	1,225,425	61,991,629	75,915,805	1.93 TB
Jul 2024	223,385	1,252,687	56,493,473	71,036,982	1.69 TB
Ago 2024	880,687	4,226,360	51,612,950	65,291,295	1.50 TB
Set 2024	823,947	3,665,787	38,646,130	49,415,994	1.15 TB
Out 2024	0	0	0	0	0
Nov 2024	0	0	0	0	0
Dez 2024	0	0	0	0	0
Total	2,838,091	17,158,563	575,753,940	698,021,252	14.39 TB

MNI PJe 1G



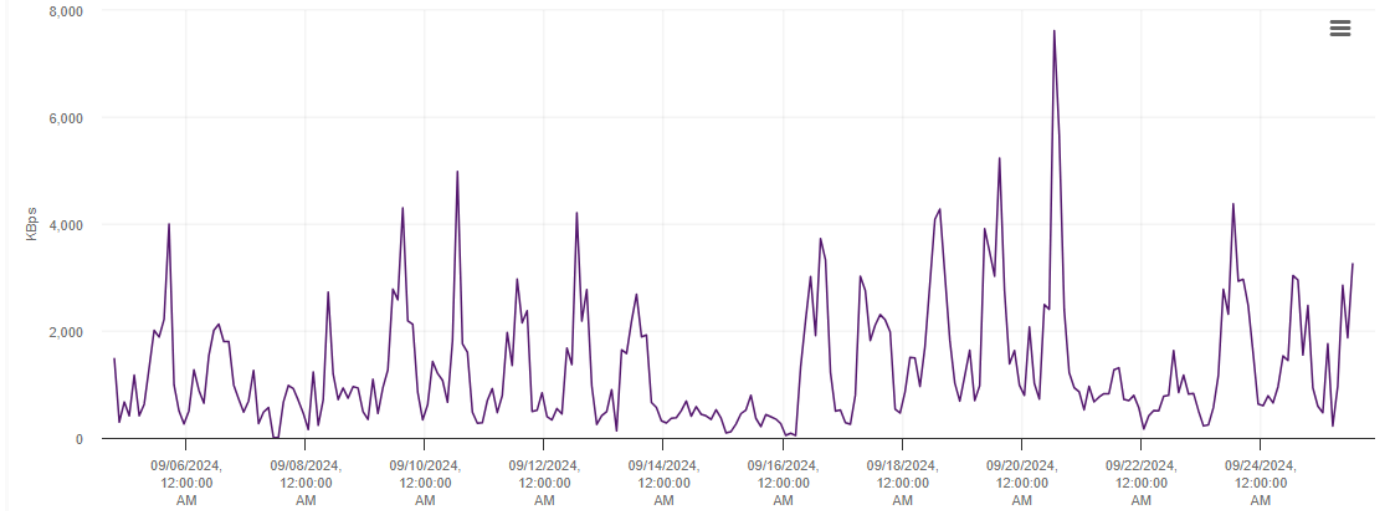
Advanced Performance

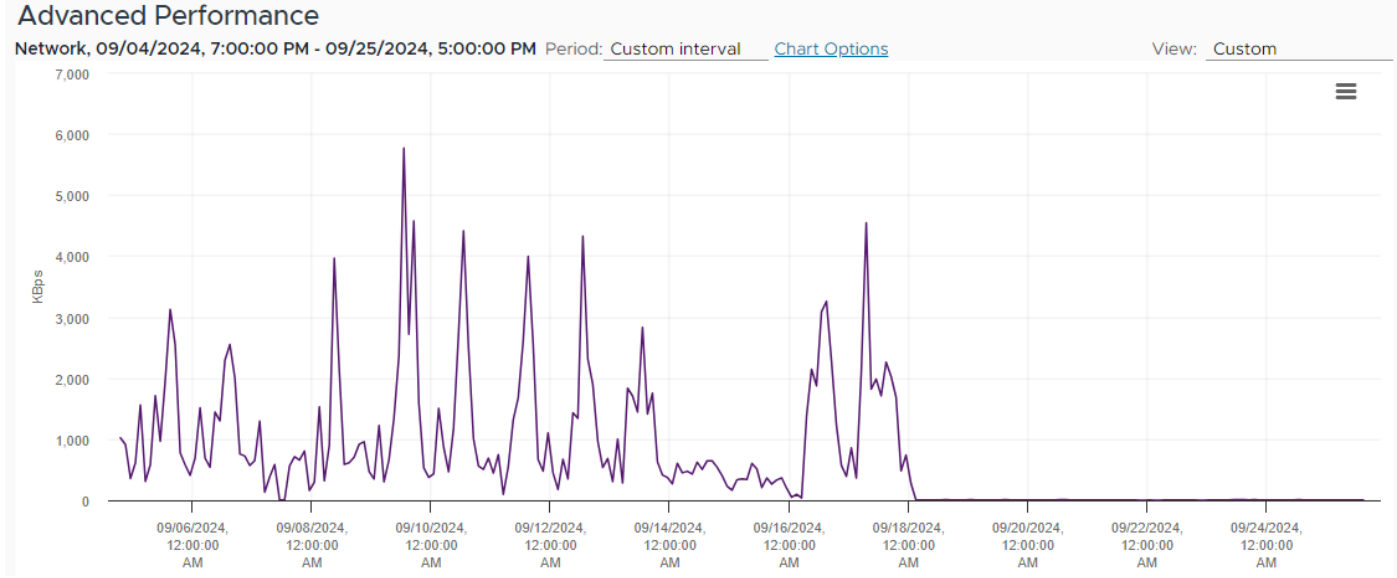
Network, 09/04/2024, 7:00:00 PM - 09/25/2024, 5:00:00 PM Period: Custom interval Chart Options View: Custom



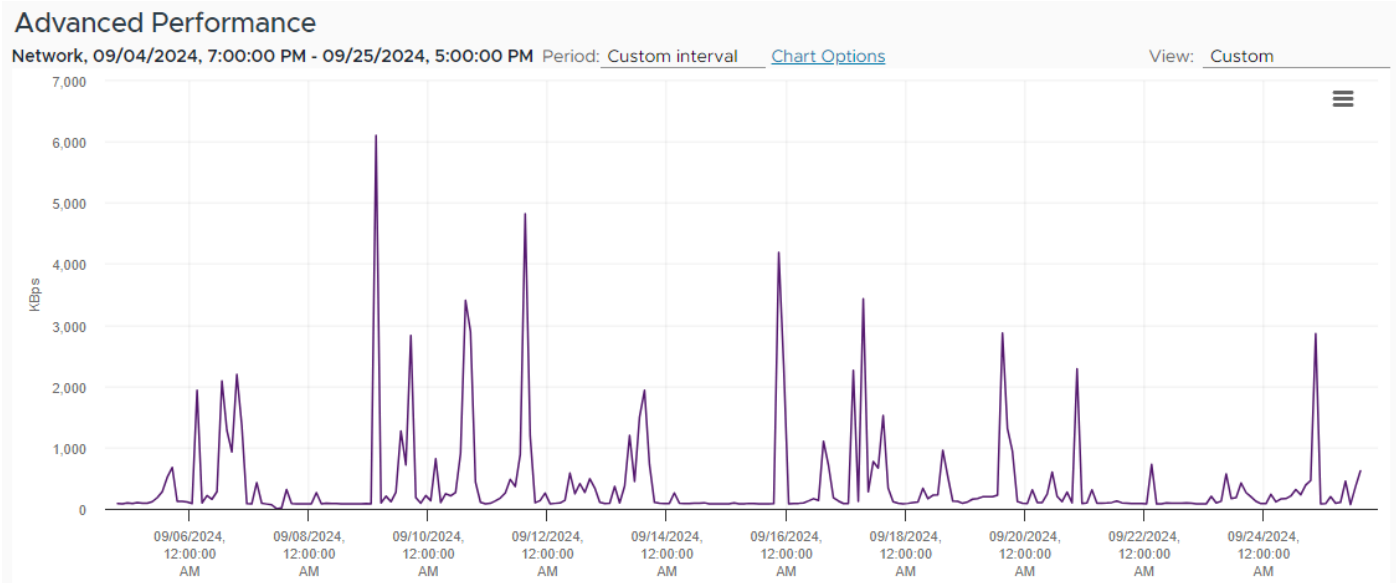
Advanced Performance

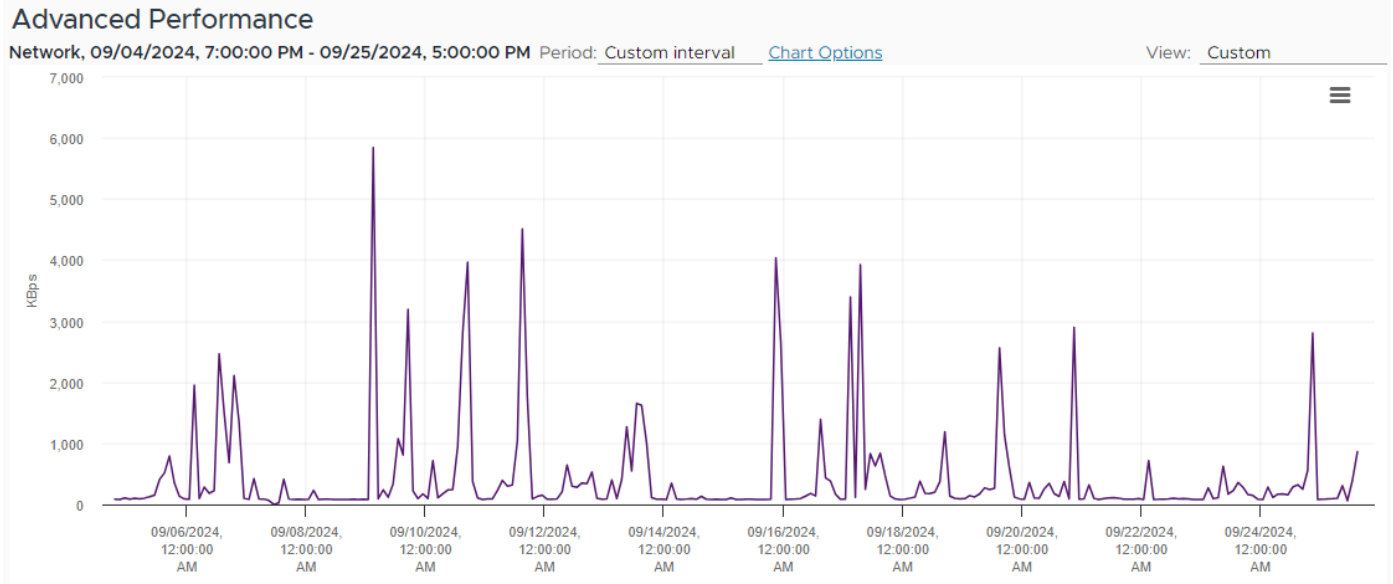
Network, 09/04/2024, 7:00:00 PM - 09/25/2024, 5:00:00 PM Period: Custom interval Chart Options View: Custom



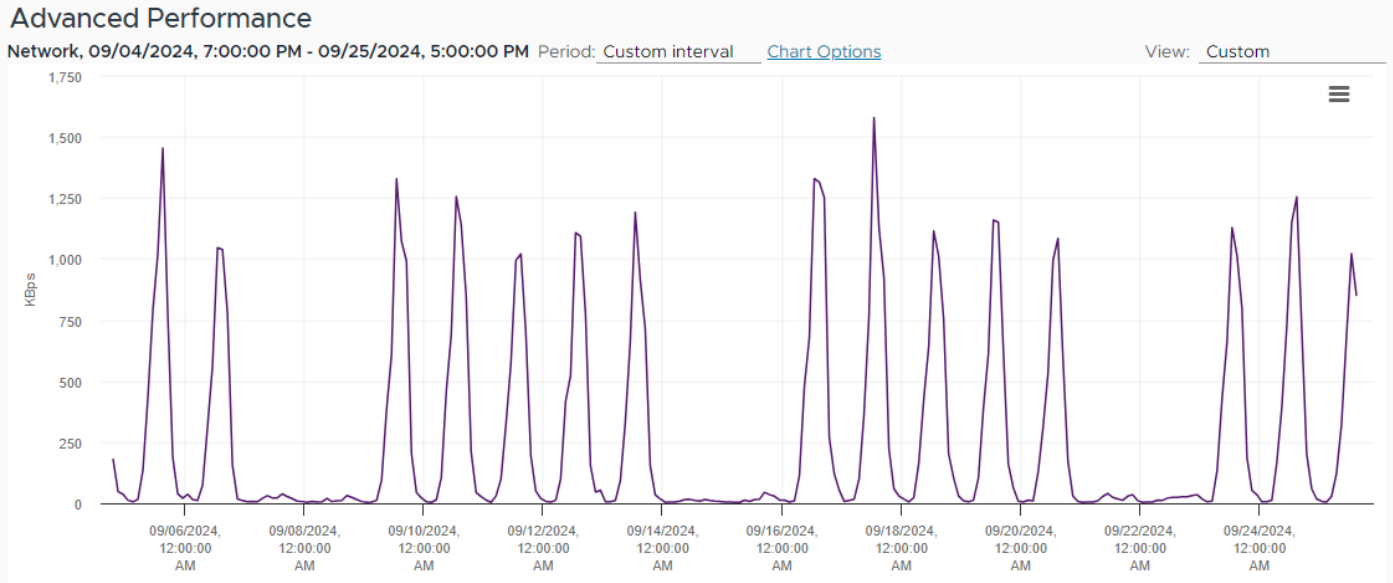

Advanced Performance
Network, 09/04/2024, 7:00:00 PM - 09/25/2024, 5:00:00 PM Period: Custom interval Chart Options View: Custom
KBps
7,000
6,000
5,000
4,000
3,000
2,000
1,000
0
09/06/2024, 12:00:00 AM
09/08/2024, 12:00:00 AM
09/10/2024, 12:00:00 AM
09/12/2024, 12:00:00 AM
09/14/2024, 12:00:00 AM
09/16/2024, 12:00:00 AM
09/18/2024, 12:00:00 AM
09/20/2024, 12:00:00 AM
09/22/2024, 12:00:00 AM
09/24/2024, 12:00:00 AM

MNI PJe 2G

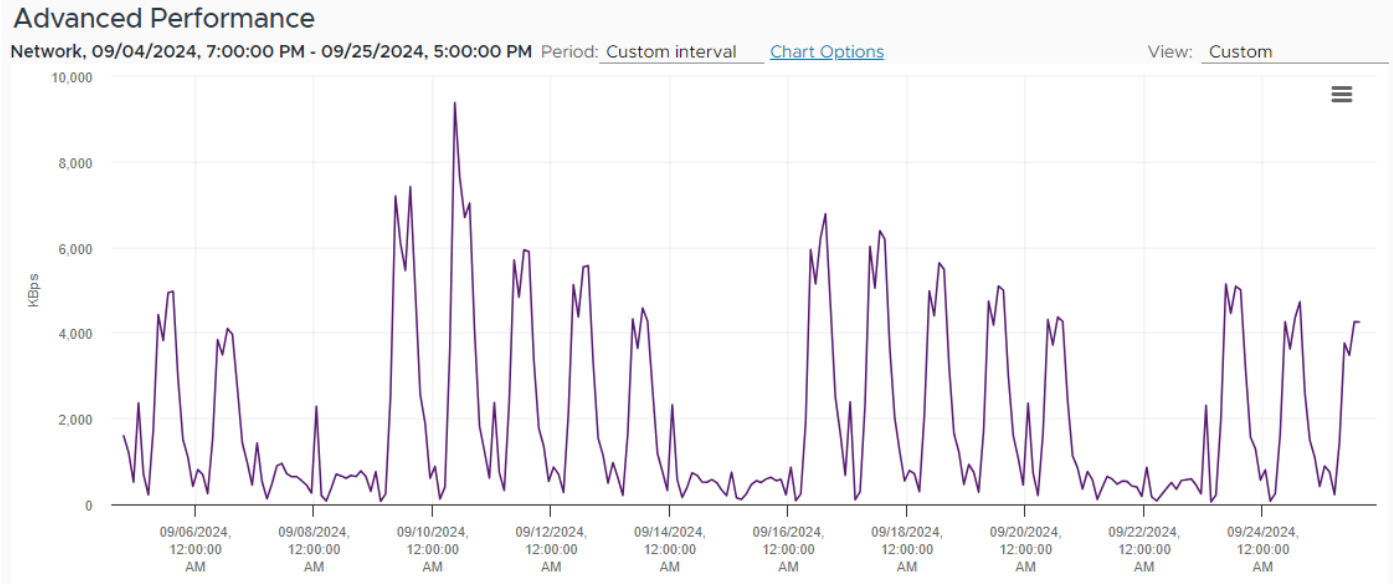

Advanced Performance
Network, 09/04/2024, 7:00:00 PM - 09/25/2024, 5:00:00 PM Period: Custom interval Chart Options View: Custom
KBps
7,000
6,000
5,000
4,000
3,000
2,000
1,000
0
09/06/2024, 12:00:00 AM
09/08/2024, 12:00:00 AM
09/10/2024, 12:00:00 AM
09/12/2024, 12:00:00 AM
09/14/2024, 12:00:00 AM
09/16/2024, 12:00:00 AM
09/18/2024, 12:00:00 AM
09/20/2024, 12:00:00 AM
09/22/2024, 12:00:00 AM
09/24/2024, 12:00:00 AM


Advanced Performance
Network, 09/04/2024, 7:00:00 PM - 09/25/2024, 5:00:00 PM Period: Custom interval Chart Options View: Custom
7,000
6,000
5,000
4,000
3,000
2,000
1,000
0
KBps
09/06/2024, 12:00:00 AM
09/08/2024, 12:00:00 AM
09/10/2024, 12:00:00 AM
09/12/2024, 12:00:00 AM
09/14/2024, 12:00:00 AM
09/16/2024, 12:00:00 AM
09/18/2024, 12:00:00 AM
09/20/2024, 12:00:00 AM
09/22/2024, 12:00:00 AM
09/24/2024, 12:00:00 AM

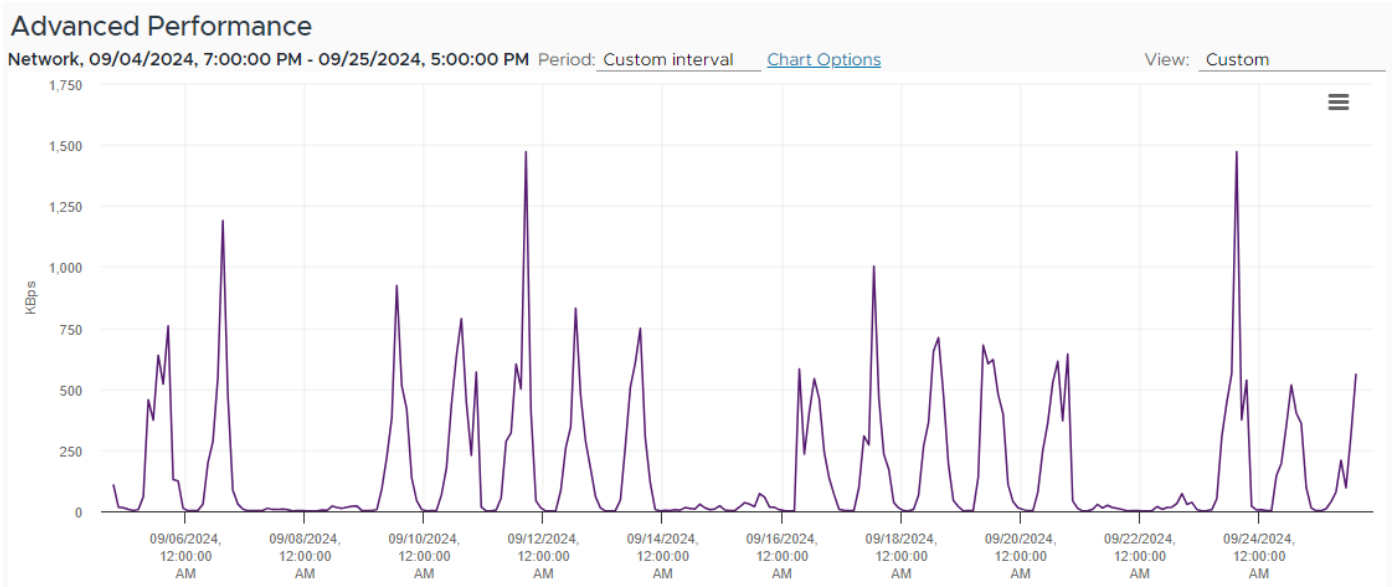
SEI


Advanced Performance
Network, 09/04/2024, 7:00:00 PM - 09/25/2024, 5:00:00 PM Period: Custom interval Chart Options View: Custom
1,750
1,500
1,250
1,000
750
500
250
0
KBps
09/06/2024, 12:00:00 AM
09/08/2024, 12:00:00 AM
09/10/2024, 12:00:00 AM
09/12/2024, 12:00:00 AM
09/14/2024, 12:00:00 AM
09/16/2024, 12:00:00 AM
09/18/2024, 12:00:00 AM
09/20/2024, 12:00:00 AM
09/22/2024, 12:00:00 AM
09/24/2024, 12:00:00 AM

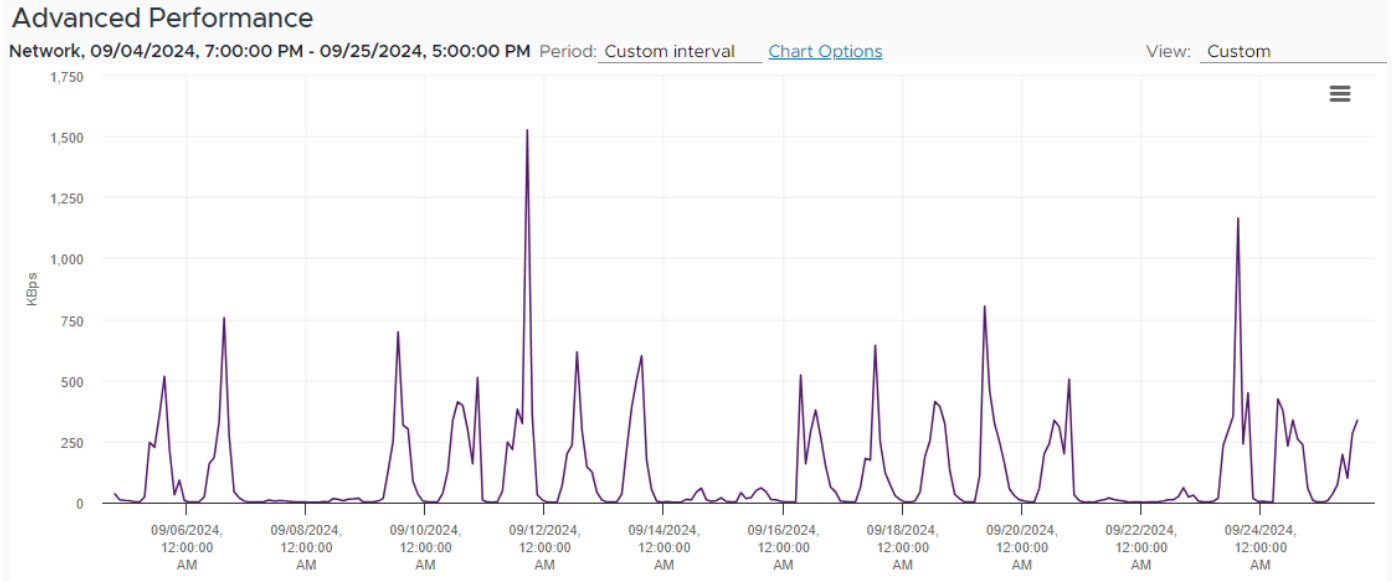
Portal



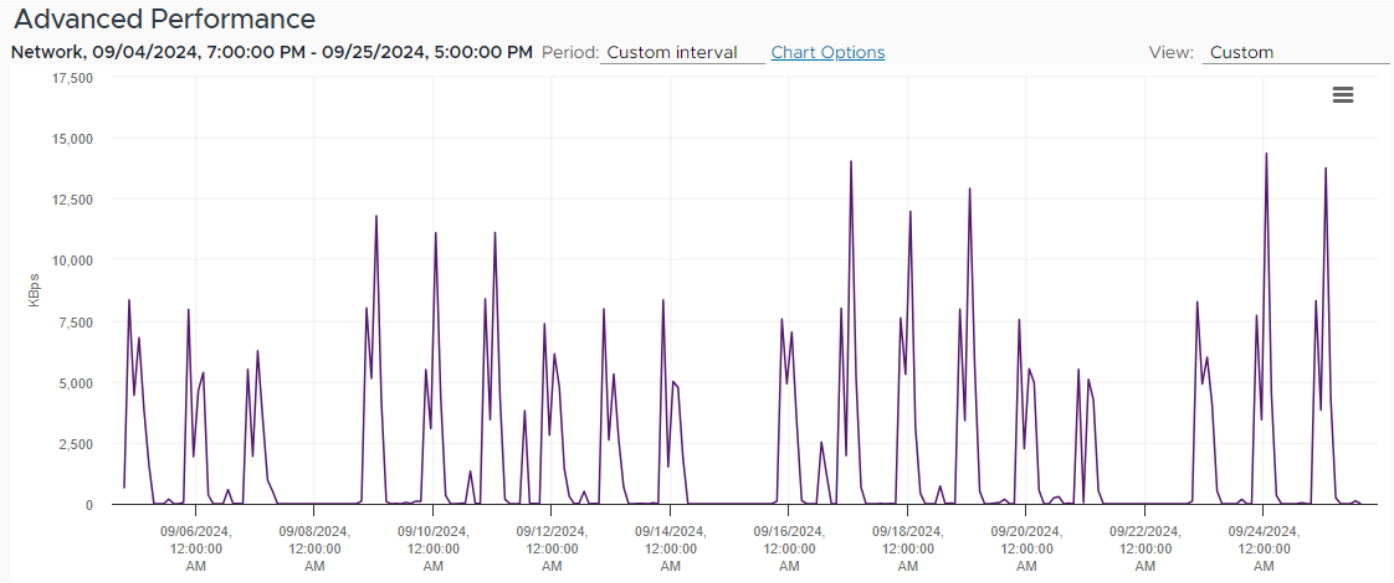
VPN



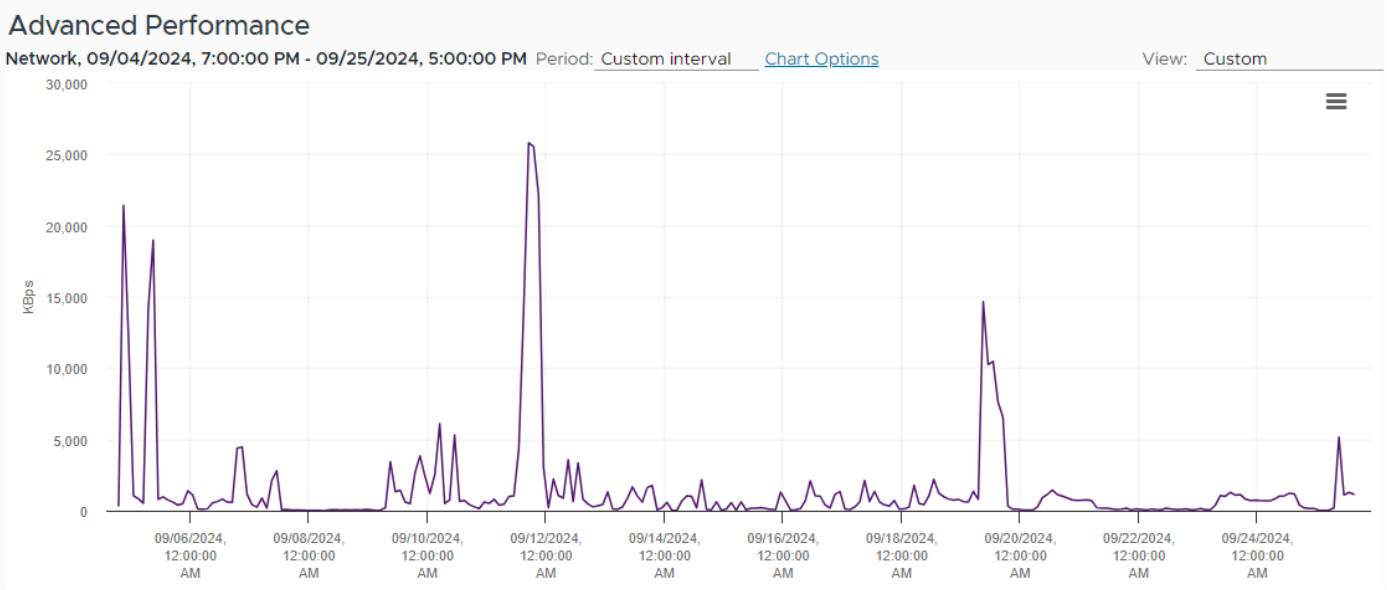
Servidor de Aplicação



Esiest



Proxy de Aplicações



VI - Estimativa do valor da contratação, acompanhada dos preços unitários referenciais, das memórias de cálculo e dos documentos que lhe dão suporte, que poderão constar de anexo classificado, se a Administração optar por preservar o seu sigilo até a conclusão da licitação

SOLUÇÕES / ÓRGÃOS	MJSP 0751481 (R$)	TRT2 0751491 (R$)	CFMV 0751498 (R$) *	STM 0751504 (R$)	TCU 0751517 (R$) *	MAP 0837732 (R$)	ARVVO 0944423 (R$)	COMPWIRE 0944460 (R$)	TELTEC 0944568 (R$)	ALTASNET 0944576 (R$)	IT ONE 0960140 (R$)	WISE IT 0960154 (R$)	MÉDIAS ESTIMADAS P/ 60 MESES (R$)
Solução em alta disponibilidade (appliance) FW	2.458.000,00	2.120.000,00				2.125.000,00			2.160.060,00	667.500,06	2.160.162,95		1.948.453,84
Licenciamentos NGFW			1.777.346,67		2.075.850,00				4.489.500,00 **	2.665.094,94	4.256.519,43 **		2.172.763,87
Instalação e Configuração		36.698,00							77.520,00	136.507,38	204.719,69		113.861,27
Suporte Técnico		23.280,00 **	868.200,00		895.000,00				1.604.040,00	1.064.996,40	552.408,00		996.928,88
Treinamento		65.210,00							102.540,00	171.665,17	86.164,63		106.394,95
Web Application Firewall - Appliance Virtual				1.200.000,00						1.158.852,57			1.179.426,29
Instalação e Configuração				74.900,00						145.129,01			110.014,51
Suporte Técnico				678.000,00						136.356,00			407.178,00
Treinamento				24.000,00						21.271,26			22.635,63
Serviço de Segurança de Borda (Security Service Edge - SSE)							14.355.000,00	10.130.400,00	14.103.420,00			29.835.842,40 **	12.862.940,00
Instalação e Configuração							122.400,00		64.800,00			1.500.000,00 **	93.600,00
Suporte Técnico									1.867.380,00			3.729.498,16 **	1.867.380,00
Treinamento									93.900,00			120.000,00	106.950,00

* Valores de contratações públicas compatibilizados conforme as quantidades necessárias ao TRF6.

** Valores desconsiderados para o cálculo da média estimada em razão da relevante disparidade em relação aos demais.

LOTES	ITENS	CATMAT / CATSER	SERVIÇOS	UNIDADES REFERENCIAIS	QUANTIDADES	VALORES MÉDIOS ESTIMADOS 60 MESES (R$)
01	01	484747	Appliances de Next Generation Firewall	Unidade	2	1.948.453,84
	02	27472	Licenciamentos para operações de Next Generation Firewall por 60 meses	Conjunto	1	2.172.763,87
	03	26972	Instalação e Configuração	Conjunto	1	113.861,27
	04	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60	996.928,88
	05	3840	Treinamento	Turma	1	106.394,95
02	06	27472	Web Application Firewall - Appliance Virtual	Unidade	1	1.179.426,29

	07	26972	Instalação e Configuração	Conjunto	1	110.014,51
	08	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60	407.178,00
	09	3840	Treinamento	Turma	1	22.635,63
03	10	27742	Serviço de Segurança de Borda (Security Service Edge - SSE)	Usuários	4.500	12.862.940,00
	11	26972	Instalação e Configuração	Conjunto	1	93.600,00
	12	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60	1.867.380,00
	13	3840	Treinamento	Turma	1	106.950,00

VII - Descrição da solução como um todo, inclusive das exigências relacionadas à manutenção e à assistência técnica, quando for o caso

NECESSIDADES DE NEGÓCIO

a) Requisitos Técnicos da Solução

1. LOTE 1. FIREWALL

1.1. Características Gerais

1.1.1. A solução deverá ser composta de hardware e software licenciado do mesmo fabricante;

1.1.2. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

1.1.3. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;

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

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

1.1.6. Os gateways de segurança, bem como a gerência centralizada, deverão suportar monitoramento através de SNMP v2 e v3;

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

1.1.8. Devem possuir homologação da Agência Nacional de Telecomunicações (ANATEL) conforme determina a Resolução nº 715, de 23 de outubro de 2019. Os documentos comprobatórios deverão ser apresentados na entrega dos equipamentos.

1.1.9. Para atendimento do Inciso III, Art. 3o do Decreto 7.174/2010, quando da entrega dos equipamentos, o licitante deverá comprovar a origem dos bens importados e apresentar comprovante de quitação dos tributos de importação a eles referentes, sob pena de suspensão do(s) pagamento(s), rescisão contratual e multa;

1.1.10. Não serão aceitas soluções em hardware de computadores pessoais (Personal Computers – PC) ou servidores, sendo obrigatório que o hardware e o software sejam do mesmo fabricante.

1.1.11. O fabricante deve ser parceiro do site www.cve.org, onde deverão estar indicados todos os CVE (Common Vulnerabilities and Exposures).

1.1.12. O fabricante deverá manter em seu site todos os CVE identificados, seu detalhamento e correções disponibilizadas.

1.1.13. A solução deve estar posicionada entre os *challengers* e *leaders* no Quadrante Mágico do Gartner mais recente para solução de Network Firewalls;

1.1.13.1. O Gartner é um dos líderes mundiais em soluções de benchmarking de tecnologia e com o maior banco de dados do setor.

1.1.14. Deverá ser apresentado, ao menos um teste de laboratório (Nacional ou Internacional) que compare o seu produto com pelo menos outros 3 (três) fabricantes, garantindo-se que o equipamento ou outro da mesma série proposta possua efetividade de segurança acima de 70%;

1.1.14.1. Para o teste especificado acima, poderá ser utilizado como referência os testes realizados pela organização sem fins lucrativos CyberRatings.org, através de sua publicação “Enterprise firewall comparative security value map q2 2023”;

1.1.15. Com o objetivo de estabelecer efetividade de segurança dos firewalls de nova geração e assegurar que o fornecedor tenha uma solução já testada e comprovada por um órgão independente de mercado, o equipamento proposto ou da mesma série proposta deverá:

1.1.15.1. Ser avaliado pela instituição NSS Labs (Network Security Services) no desempenho do Next Generation Firewall Comparative Analysis mais recente e deve constar no “Security Value Map” acima de 90% (noventa por cento); OU

1.1.15.2. Ser avaliado pela instituição NetSecOpen; OU

1.1.15.3. Ser avaliado pela instituição Miercom Certified Perfomance Verified; OU

1.1.15.4. Ser avaliado pela instituição Miercom Certified Secure.

1.2. Capacidades e Quantidades - Solução em Appliance de Segurança de Perímetro de Próxima Geração

1.2.1. Throughput de, no mínimo, 15 Gbps (Threat Protection/Prevention SEM SSL/TLS) e no mínimo 5.8 Gbps(Threat Protection/Prevention COM SSL/TLS), com as seguintes funcionalidades habilitadas:

1.2.1.1. Firewall;

1.2.1.2. Detecção e Prevenção de intrusão (IDS/IPS);

1.2.1.3. Controle de aplicação;

1.2.1.4. Filtro de URL;

1.2.1.5. Antivírus;

1.2.1.6. Anti-spyware;

1.2.1.7. Anti-phishing;

1.2.1.8. Bloqueio de arquivos e logs;

1.2.1.9. Prevenção de ameaças avançadas de dia zero;

1.2.1.10. Inspeção SSL/TLS;

1.2.2. O fabricante deve possuir documentação pública, descrevendo o perfil de tráfego;

1.2.3. A documentação deverá ser específica para o modelo ofertado, sob pena de desclassificação;

1.2.4. Suporte a, no mínimo, 5M (cinco milhões) de conexões simultâneas;

1.2.5. Suporte a, no mínimo, 250.000 (Duzentos e cinquenta mil) novas conexões por segundo;

1.2.6. Throughput de, no mínimo, 11 (onze) Gbps, no mínimo, para conexões VPN;

1.2.7. Suportar e estar licenciado para acesso remoto Client-to-site ilimitado ou com a licença de maior capacidade;

1.2.8. Fonte de alimentação redundante e hot-swappable;

1.2.9. O firewall deverá possuir memória suficiente para aguentar a performance exigida no edital durante todo o tempo do contrato;

1.2.10. No mínimo, 12 (doze) interfaces de rede 10Gbps SFP+;

1.2.11. No mínimo, 04 (quatro) interfaces de rede 10/100/1000;

1.2.12. No mínimo, 02 (duas) interfaces de 40G QSFP+;

1.2.13. Todas as interfaces devem vir acompanhadas do respectivo transceiver padrão Multimodo;

1.2.14. Possuir 1 (uma) interface de rede para sincronismo;

1.2.15. Possuir 1 (uma) interface de rede dedicada ao gerenciamento, não sendo permitido utilizar qualquer outra interface para exercer a função de gerenciamento do equipamento;

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

1.2.17. Cada um dos appliances da plataforma de proteção de rede deve possuir discos Solid State Drive (SSD) redundantes com no mínimo 480 GB de capacidade de armazenamento para o Sistema Operacional;

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

1.2.19. Suporte a RFC 4291 de Arquitetura de endereçamento IPv6;

1.2.20. Deve suportar Dual stack ipv4/ipv6 e NAT64;

1.2.21. Deve suportar NAT64 e NAT46;

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

1.2.23. Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP v4 e v6 sem duplicação da base de objetos e regras;

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

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

1.3. Funcionalidades de Firewall

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

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

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

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

1.3.5. Realizar upgrade via SCP ou SFTP e https via interface WEB;

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

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

1.3.6.2. Deverá suportar VXLAN;

1.3.7. Deve suportar os seguintes tipos de NAT:

1.3.7.1. Nat dinâmico (Many-to-1);

1.3.7.2. Nat estático (1-to-1);

1.3.7.3. Tradução de porta (PAT);

1.3.7.4. NAT de Origem;

1.3.7.5. NAT de Destino;

1.3.7.6. Suportar NAT de Origem e NAT de Destino simultaneamente;

1.3.8. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

1.3.9. As regras de NAT devem suportar “hit count” para monitorar a quantidade de conexões que deram matches em cada regra;

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

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

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

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

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

1.3.15. Suportar OSPF graceful restart;

1.3.16. Deve suportar roteamento ECMP (equal cost multi-path);

1.3.17. Para o ECMP, a solução deve suportar o balanceamento do roteamento de forma simultânea usando os seguintes parâmetros Origem, Destino, Porta de Origem, Porta de Destino e Protocolo;

1.3.18. Autenticação integrada via Kerberos;

1.3.19. A solução deve possuir mecanismo para dedicar processamento no equipamento de segurança para funções/ações de gerenciamento mesmo que o equipamento esteja com alto processamento de CPU, de forma a evitar a falta de acesso do administrador para qualquer mitigação de falha e aplicação de política para solução de problema.

1.3.20. As regras Firewall devem suportar "hit count" para monitorar a quantidade de conexões que deram matches em cada regra;

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

1.3.22. A solução deve permitir o agendamento de instalação de políticas para serem aplicadas em horários pré-definidos através da console centralizada **ou** permitir salvar as configurações das políticas para serem aplicadas em horários pré-definidos;

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

1.3.24. Deverá suportar redundância e balanceamento de links, tendo capacidade a no mínimo 3 links de internet;

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

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

1.4. Funcionalidades de Filtro de Conteúdo WEB

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

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

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

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

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

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

1.4.5.2. Reconhecer pelo menos 4.500 (quatro mil e quinhentas) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, *update* de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

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

1.4.7. Para inspeção SSL, ou HTTPS Inspection, a solução deve oferecer suporte ao HTTP/3 ou Perfect Forward Secrecy (conjuntos de cifras PFS, ECDHE);

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

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

1.4.10. A fim de otimização de tempo operacional dos administradores, a solução deverá possuir pelo menos 30 categorias ou subcategorias de aplicações WEB pré-definidas pelo fabricante;

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

1.4.12. Possuir mecanismo de controle de aplicação web e URL com configuração de bloqueio e liberação da aplicação principal e/ou as suas subcategorias. Quando o administrador da solução desejar bloquear apenas as sub-categorias do facebook, como facebook chat, vídeo, game, compartilhamento de arquivos ou outros. Ou seja, não deve ser bloqueado toda a categoria como "Facebook" ou "Redes sociais" que também pode implicar o bloqueio não só do Facebook, mas também bloqueará tudo que estiver relacionado às redes sociais, como LinkedIn, Twitter , YouTube, etc..

1.4.12.1. A solução precisa ser baseada em bloqueio de aplicações WEB que a própria base possui, assim a inspeção ocorrerá em camada 7 analisando o payload do pacote;

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

1.4.14. Atualizar a base de assinaturas de aplicações automaticamente;

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

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

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

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

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

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

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

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

1.4.23. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs atráves da integração com serviços de diretório, autenticação via Active Directory e base de dados local;

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

1.4.25. Suportar armazenamento, na própria solução ou na plataforma de gerencia local, de URLs, evitando delay de comunicação/validação das URLs;

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

1.4.27. Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja solução de software livre;

1.4.28. Suportar a criação de categorias de URLs customizadas;

1.4.29. Suportar a exclusão de URLs do bloqueio, por categoria;

1.4.30. Permitir a customização de página de bloqueio;

1.4.31. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede;

1.4.32. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius ou APIs ou Syslog, para a identificação de endereços IP e usuários;

1.4.33. Deve permitir o controle, sem instalação de cliente de software, em máquinas/computadores que solicitem saída à internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no Firewall (Captive Portal);

1.4.34. A solução deverá implementar uma análise avançada de URL em tempo real enviando a URL para o serviço de análise em cloud e não somente fazer a consulta em base local;

1.4.35. A filtragem de URL em tempo real deverá ser ativada por meio de filtragem de URL.

1.5. Funcionalidades de Prevenção de Ameaças

1.5.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus, Anti-Malware e Anti Phishing integrados no próprio equipamento de firewall;

1.5.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos;

1.5.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware e Anti-Phishing quando implementado em alta disponibilidade ativo/passivo;

1.5.4. Deve suportar granularidade nas políticas de Antivírus, Anti-Phishing e Anti-malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

1.5.5. A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo ou gerenciado automaticamente pelo SO;

1.5.6. Deverá possuir os seguintes mecanismos de inspeção de IPS:

1.5.6.1. Análise de padrões de estado de conexões, análise de decodificação de protocolo;

1.5.6.2. Análise para detecção de anomalias de protocolo;

1.5.6.3. IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

1.5.7. Detectar e bloquear a origem de portscans;

1.5.8. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

1.5.9. Possuir assinaturas para bloqueio de ataques de buffer overflow;

1.5.10. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;

1.5.11. Suportar bloqueio de arquivos por tipo;

1.5.12. Identificar e bloquear comunicação com botnets;

1.5.13. Deve suportar referência cruzada com CVE;

1.5.14. Em cada proteção de segurança, deve estar incluso informações como:

1.5.14.1. Código CVE (Common Vulnerabilities and Exposures), não sendo aceito outro código de referência;

1.5.14.2. Severidade;

1.5.14.3. Tipo de ação a ser executada;

1.5.15. O IPS deve fornecer um mecanismo automatizado para ativar ou gerenciar novas assinaturas vindas de atualizações.

1.5.16. O IPS deve suportar exceções de rede com base na origem, destino, serviço ou uma combinação dos três.

1.5.17. O IPS deve incluir um modo de solução de problemas que defina o perfil em uso para detectar apenas, sem modificar as proteções individuais.

1.5.18. O administrador deve poder ativar automaticamente novas proteções, com base em parâmetros configuráveis (impacto no desempenho, gravidade da ameaça, nível de confiança, proteção do cliente, proteção do servidor)

1.5.19. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

1.5.19.1. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;

1.5.20. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS através da console de gerência centralizada;

1.5.21. Na própria interface de gerência, a solução de IPS deverá apresentar sumário de todos os equipamentos que estão sendo gerenciados;

1.5.22. A solução de IPS, deve possuir mecanismo de análise baseado nas conexões realizadas para as aplicações, que aponta quais assinaturas que estão em modo detecção devem ser alterada para modo prevenção, assim evitando qualquer tipo de ataque para aplicações que estão expostas no ambiente.

1.5.23. O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados na funcionalidade de IPS;

1.5.24. A solução deverá possuir pelo menos dois perfis pré-configurados pelo fabricante que permitam sua utilização assim que o equipamento for configurado;

1.5.25. A solução deve permitir que o administrador possa configurar quais métodos e comandos HTTP são permitidos e quais são bloqueados.

1.5.26. Deve incluir proteção contra vírus em conteúdo ActiveX e applets Java e worms;

1.5.27. Solução deve proteger contra os ataques do tipo DNS Cache Poisoning, e impedir que os usuários acessem endereços de domínios bloqueados;

1.5.28. O gerenciamento centralizado via interface gráfica deve possibilitar a configuração de captura dos pacotes por regras individuais, visando aperfeiçoar o desempenho do equipamento;

1.5.29. A solução de IPS deve possuir engine com determinação de forma automática de qualquer nova assinatura que for baixada na base local;

1.5.29.1. Deverá atuar em modo de prevenção ou detecção, de forma a evitar qualquer tipo de alteração na base de assinatura atual;

1.5.30. O antivírus deve oferecer suporte à verificação de links dentro de e-mails.

1.5.31. A solução de anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede quando usuário estiver conectado com ambiente externo malicioso.

1.5.32. A solução deve permitir criar regras de exceção de acordo com a proteção, a partir do log visualizado na interface gráfica da gerência centralizada;

1.5.33. Para melhor administração a solução deve possuir a granularidade na classificação das proteções de IPS através de: severidade, sistema operacional (minimamente Windows e Linux), target (cliente e servidor); ou nível de confiança da proteção, impacto da performance, referência de indústria terceira e status de download recente;;

1.5.34. A solução deve permitir a criação de White list baseado no MD5 do arquivo;

1.5.35. Os eventos devem identificar o país de onde partiu a ameaça;

1.5.36. Suportar rastreamento de vírus em arquivos pdf;

1.5.37. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);

1.5.38. Possuir a capacidade de prevenção de ameaças não conhecidas;

1.5.39. Em caso de falha no mecanismo de inspeção do Antivírus, deve ser possível configurar se as conexões serão permitidas ou bloqueada;

1.5.40. A solução de Antivírus e Antimalware deve funcionar de forma independente, ou seja, caso sejam desabilitadas, elas não podem causar a interrupção de outras funcionalidades de segurança como prevenção de ameaças avançadas (zero-day);

1.5.41. A solução Antivírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS/SMB, de forma a conter malwares se espalhando horizontalmente pela rede;

1.5.42. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;

1.5.43. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

1.5.44. Deverá possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos, sejam resolvidas pelo Firewall com endereços previamente definidos, para interceptar a comunicação e bloquear o acesso do usuário.

1.5.45. A solução de Antimalware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede.

1.5.46. A solução deve possuir funcionalidade de identificação de bloqueio de trafego malicioso comunicando com C&C (command & Control);

1.5.47. A solução Antivírus deverá suportar a análise de links no corpo de e-mails.

1.5.48. Modelos de deep learning em linha para prevenir tráfego C2 desconhecido e evasivo de ferramentas como Cobalt Strike e Empire;

1.5.49. Modelos de machine learning baseados na nuvem, atualizados regularmente, para prevenir explorações desconhecidas de injeção de comandos e injeção de SQL;

1.5.50. Bloqueio de ataques de malware na camada de rede com detecções baseadas em assinaturas em linha;

1.5.51. Assinaturas personalizadas para vulnerabilidades de software e ataques de command-and-control;

1.5.52. Análise baseada em heurísticas, decodificação de protocolos, proteção contra anomalias de protocolo e assinaturas de vulnerabilidades personalizadas;

1.5.53. Inspeção e classificação do tráfego, detectando e bloqueando malware e exploits de vulnerabilidades em uma única passagem;

1.5.54. Uso de AI, aprendizado de máquina e deep learning para detecção precisa de variantes avançadas de malware;

1.6. Funcionalidades de Controle de Qualidade de Serviço

1.6.1. Suportar a criação de políticas de QoS por: endereço de origem, endereço de destino e por porta;

1.6.2. O QoS deve possibilitar a definição de classes por: Banda garantida, banda máxima e fila de prioridade;

1.6.3. Disponibilizar estatísticas em tempo real para classes de QoS;

1.6.4. A solução deve permitir, por aplicação, o encaminhamento do tráfego para diferentes links de Internet, sejam eles locais ou remotos, deve suportar múltiplos links de acesso como MPLS, Internet Banda Larga, LTE (Private or Public APN) e Satélite;

1.6.5. Deve possibilitar a utilização de configuração inteligente de acessos WAN IP ativos-ativos sem a necessidade de switch para agregação WAN, ou seja, distribuir o tráfego simultaneamente pelos N acessos conectados e não apenas na configuração dos acessos principal e backup;

1.6.6. Medir parâmetros de rede jitter, perda de pacotes e latência em tempo real;

1.6.7. Se houver necessidade de saída internet do ponto remoto, deve ser possível selecionar por tipo de aplicativo;

1.6.8. Deve permitir a comunicação indireta entre localidades por meio de uma topologia “hub and spoke”;

1.6.9. Deve balancear o tráfego de aplicativos em vários links simultaneamente;

1.6.10. Redistribuição do tráfego balanceado, de forma inteligente, tendo em conta o congestionamento da largura de banda, entre os links utilizados, em caso de falhas nestes links, ou de acordo com as políticas de qualidade pré-definidas;

1.6.11. Habilitar a mesma interface WAN para enviar tráfego simultaneamente por meio de túneis IPSec SD-WAN e nativamente fora dos túneis via underlay;

1.6.12. Habilitar a criação de políticas de negócios para controlar o padrão de redirecionamento de tráfego e aplicar qualidade de serviço;

1.6.13. Suportar políticas inteligentes usando configuração padrão de fábrica que executem redirecionamento automático e imposição de QoS de voz, vídeo e tráfego transacional;

1.6.14. Suportar o redirecionamento do tráfego de internet de pontos remotos para um ponto de internet centralizado, usando políticas por aplicativo;

1.6.15. Redirecionamento condicionado do tráfego de internet em caso de falha do link de internet local ou do link remoto centralizado, utilizando políticas por aplicativo;

1.6.16. Suporte simultâneo ao redirecionamento do tráfego da Web de alguns aplicativos para a Internet centralizada, outros aplicativos para a Internet local e outros aplicativos para inspeção avançada de segurança na nuvem;

1.6.17. Implementar o conceito de perfis de configuração e grupos de objetos para automatizar o processo de implementação de políticas em grande escala;

1.6.18. Usar probes artificiais baseadas em icmp, udp ou tcp para medir a qualidade da rede percebida pelo tráfego do usuário, medindo no minimo jitter, latencia e perda de pacotes;

1.6.19. Capacidade de realizar agregação de largura de banda automaticamente entre links de diferentes velocidades, levando em consideração o uso total da largura de banda de cada link sem causar congestionamento em links de baixa velocidade;

1.6.20. Habilitar a configuração de backup do link, ou seja, um link de backup só deve ser ativado quando o link principal falhar;

1.6.21. Implementar um mecanismo de proteção de variação de latência (jitter) mesmo que a degradação esteja em todos os links, para proteger o tráfego em tempo real (voz e vídeo)de forma a priorizar este tráfego em conjunto com controle de qualidade do SD-Wan;

1.6.22. Garantir o desempenho de aplicativos em um cenário de link de transporte duplo quando ambo os links estão degradados simultaneamente;

1.6.23. Possuir um mecanismo de priorização (QoS) para proteger o tráfego de aplicativos clientes prioritários quando houver congestionamento em pontos remotos;

1.6.24. Deve automatizar o reconhecimento dos melhores níveis de SLA de rede com base no tipo de tráfego seja áudio, vídeo ou transacional;

1.6.25. O console de gerenciamento deve informar o status operacional (UP/DOWN/SPEED) das interfaces LAN e WAN;

1.6.26. O console de gerenciamento deve informar o status operacional de cada dispositivo que faz parte da rede para operacionalidade;

1.6.27. Realizar medições de “Latência”/”Jitter”/”Queda de pacotes” em cada um dos túneis SDWAN independentemente, na direção de transmissão ou recepção;

1.6.28. O Orquestrador pode estar na Nuvem ou até mesmo ser instalado em um servidor dedicado ou virtualizado, utilizando uma máquina virtual;

1.6.29. No caso do Orchestrator estar na nuvem, a administração de atualizações, gerenciamento de alta disponibilidade e hardening do plano de gerenciamento deve ser realizada pelo fabricante da solução.

1.7. Funcionalidades de VPN

1.7.1. Suportar VPN Site-to-Site e Cliente-To-Site;

1.7.2. Suportar IPSec VPN;

1.7.3. A solução deve suportar Autoridade Certificadora Interna e Externa (de terceiros);

1.7.4. Suportar SSL VPN;

1.7.5. A VPN IPSEc deve suportar:

1.7.5.1. Algoritmos de criptografia 3DES, AES 128 e 256;

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

1.7.5.3. Algoritmo Internet Key Exchange (IKE) v1 e v2;

1.7.5.4. Autenticação via certificado IKE PKI;

1.7.5.5. Autenticação MD5, SHA-1, SHA-384,SHA-256, SHA-512;

1.7.6. A VPN SSL deve suportar:

1.7.6.1. Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

1.7.6.2. A funcionalidade de VPN SSL deve ser atendida com ou sem o uso de agente;

1.7.6.3. Suportar configuração de conformidade para acesso do usuário via portal SSL ou cliente na máquina do usuário;

1.7.6.4. Atribuição de endereço IP nos clientes remotos de VPN;

1.7.6.5. Atribuição de DNS nos clientes remotos de VPN;

1.7.6.6. Dever permitir criar políticas para tráfego dos clientes remotos conectados na VPN SSL.

1.7.7. A solução deve possuir checagem de conformidade e verificar, no mínimo, as seguintes informações no cliente remoto: sistema operacional e patches instalados, antivírus, firewall no host, chaves de registros e processos ativos;

1.7.8. A solução deve permitir bloquear o acesso do usuários aos recursos via VPN caso o usuário não esteja em conformidade com a verificação dos parâmetros configurados;

1.7.9. Suportar autenticação via AD/LDAP, certificado e base de usuários local;

1.7.10. A solução deve permitir a integração da ferramenta com provedores de identidade, atraves de SAML, para autenticação dos usuários remotos conectados via VPN;

1.7.11. Suportar leitura e verificação de CRL (certificate revocation list);

1.7.12. A tecnologia de VPN Client to Server deverá ser instalada na plataforma: iOS 10 ou superior e Android;

1.7.13. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows 7, Windows 10/11 e MacOS X.

1.8. Solução para Proteção Contra Ameaças Avançadas - Zero Day

1.8.1. A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT;

1.8.2. A solução deverá ser composta por hardware e software específicos (appliance) com sistema operacional especializado em sua versão mais atualizada ou nuvem do proprio fabricante que possui o conceito de sandboxing para prevenção de ataques zero-day;

1.8.3. Não será aceito soluções que dependa da estrutura de hypervisor do contratante para a analise de ameaças de dia zero, como Vmware ESXi, Microsoft HyperV, entre outros;

1.8.4. Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS), FTP e E-mail (SMTP/TLS) durante análise completa do arquivo no ambiente sandbox, sem que o mesmo seja entregue parcialmente ao cliente.

1.8.5. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;

1.8.6. Implementar, identificar e bloquear malwares de dia zero em links de e-mail e URLs conhecidas;

1.8.7. Ameaças trafegadas em protocolo SMTP, de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;

1.8.8. A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows 7, Windows 10/11, MacOS, Android, Linux assim como Office;

1.8.9. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas antes de entregar este arquivo para o cliente;

1.8.10. O conteúdo enviado para a solução de Sandboxing deverá ser feito automaticamente, sem a necessidade da interação do usuário/administrador para que o processo de análise seja realizado;

1.8.11. Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, dias da semana ou dias do mês assim como o período de cada atualização;

1.8.12. Toda análise dos arquivos deverá ser realizada em ambiente controlado Sandboxing em nuvem ou on-premisse em equipamentos dedicados para este fim do mesmo fabricante da solução ofertada.. Não serão aceitas soluções em servidores genéricos ou software livre;

1.8.13. A funcionalidade de prevenção de ameaças avançadas deve ser habilitada e funcionar de forma independente das outras funcionalidades de segurança;

1.8.14. Toda análise deverá ser realizada em nuvem do próprio fabricante ou equipamento on-premisse do mesmo fabricante da solução;

1.8.15. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF acima de 10 Mb;

1.8.16. Deve implementar análise em sandbox, detecção e bloqueio de malwares em arquivos executáveis, DLLs, ZIP e criptografados em SSL;

1.8.17. Deve implementar análise em sandbox, detecção e bloqueio de malwares em arquivos java (.jar e class);

1.8.18. A solução deve suportar inspeção para o protocolo SMBv3;

1.8.19. O relatório das emulações deve apresentar de maneira detalhada as atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado;

1.8.20. Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas;

1.8.21. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;

1.8.22. Capacidade de análise, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, seven-z, exe, dll, rtf, csv, scr, todos os tipos de arquivos do Microsoft Office, arquivos do Mac OS X, arquivos do Linux(ELF), arquivos do Android Package Kit (APK), arquivos do Adobe Flash, arquivos de script(BAT,JS,VBS,PS1,script do Shell e HTA), análise de links em mensagens de e-mail e arquivos criptografados (TLS/SSL);

1.8.23. Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real e o bloqueio deve ser imediato, não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;

1.8.24. Possibilitar remoção de conteúdo ativo dinâmicos como macros, URLs, Java scripts e outros dos arquivos baixados, permitindo o download do arquivo original caso ele não seja malicioso;

1.8.25. A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;

1.8.26. A solução deve possuir mecanismo para identificar sites conhecidos e desconhecidos como phishing, analisando em tempo real a URL acessada.

1.8.27. A solução deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas informações em sites classificados como phishing;

1.8.28. O Mecanismo de classificação de anti-phishing deve atuar sem a necessidade de instalação de agente na máquina do usuário;

1.8.29. Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:

1.8.29.1. Número de arquivos emulados;

1.8.29.2. Número de arquivos com malware;

1.8.30. A solução de prevenção de ameaças avançada, deve possuir capacidade de apresentar em seus logs, visibilidade de acordo com o framework ATT&CK Mitre Matrix, pontuando características de táticas e técnicas de acordo com a ameaça detectada/bloqueada pela solução. Caso a solução não possua determinada capacidade, poderá ser integrada com outra solução de mercado, não sendo ela soluções abertas;

1.8.31. A solução deve prover informação, seja por meio de relatório ou log, sobre as seguintes situações:

1.8.31.1. Quantidade arquivos emulados e ações aplicadas OU o tamanho máximo do arquivo emulado seja excedido;

1.8.31.2. Classificar dos arquivos minimamente com os tipos (limpos, suspeitos e maliciosos) ou o tempo máximo de emulação seja excedido.

1.9. Módulo de Gerência

1.9.1. A solução de gerência deverá ser separada dos gateways de segurança, que irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas neste documento, exceto Sandbox que poderá ser gerenciado individualmente;

1.9.2. Deve ser compatível com VMware ESXi com espaço de armazenamento para LOGs de no mínimo, 200GB/LOG/DIA de ingestão;

1.9.3. Caso a solução possua licenças relacionadas a capacidade de log indexados e armazenamento, deve ser ofertado, no mínimo, 200GB/log/dia de ingestão;

1.9.4. Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução;

1.9.5. Deve fornecer consultas de logs, geração de relatório das funcionalidades de segurança que estão ativadas nos NGFWs e telas de apresentação onde consta todo os principais eventos das funcionalidades de controle de aplicação web, filtro URL, prevenção de ameaças (IPS, Antivírus, Anti-phishing, Anti-Malware e Sandboxing);

1.9.6. Deve possuir solução de gerenciamento e administração centralizado, possibilitando o gerenciamento de diversos equipamentos de proteção de rede do mesmo fabricante desde que não sejam software livre;

1.9.7. O módulo de gerência deve ser capaz de gerenciar e administrar todas as soluções descritas neste termo podendo estar em uma gerência a parte;

1.9.8. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;

1.9.9. Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento;

1.9.10. O gerenciamento da solução deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS);

1.9.11. Todos os logs da solução devem ser indexados e seu licenciamento deve ser o de maior capacidade.

1.9.12. O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores;

1.9.13. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

1.9.14. Suportar criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração;

1.9.15. Suportar backup das configurações e rollback de configuração para a última configuração salva;

1.9.16. Suportar validação de regras antes da aplicação;

1.9.17. Suportar validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

1.9.18. Deve permitir a visualização dos logs de uma regra específica em tempo real e na mesma tela de configuração da regra selecionada;

1.9.19. Deve possibilitar a integração com outras soluções de SIEM de mercado desde que não sejam software livre;

1.9.20. Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

1.9.21. Deve apresentar eventos em um único portal (dashboard) e geração de relatório de todas as funcionalidades de segurança que estão ativadas nos GW's de segurança, sendo que deve possuir relatório e telas de apresentação onde consta todo os principais eventos das funcionalidades de controle de aplicação web, filtro URL, prevenção de ameaças (IPS, Antivírus, Anti-Malware, Anti-phishing e Sandboxing);

1.9.22. A solução deve permitir o login de múltiplos usuários administradores simultâneos com perfil de escrita, possibilitando agilidade e rapidez no gerenciamento pelo grupo de administradores da solução.

1.9.23. A solução deve permitir a integração da ferramenta com provedores de identidade para autenticação dos administradores da solução via SAML 2.0;

1.9.24. A solução deve permitir revisar e aprovar alterações de políticas de segurança feitas por outros administradores.

1.9.25. A solução deve permitir criar perfis de administradores para realizar revisão/alteração das políticas de segurança, com no mínimo, os perfis de aprovador e solicitante.

1.9.26. A solução deverá enviar a solicitação de aprovação de políticas de segurança por pelo menos uma das seguintes formas, Email, Requisição WEB ou Scripts.

1.9.27. Permitir criação de relatórios customizados via interface gráfica, sem necessidade de conhecer linguagens de banco de dados podendo utilizar de datasets pré customizados pelo fabricante;

1.9.28. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware), e URLs que passaram pela solução;

1.9.29. Deve ser possível exportar os logs em CSV ou TXT;

1.9.30. O visualizador de log deve ter um recurso de pesquisa de texto livre;

1.9.31. Deve possibilitar a geração de relatórios de eventos no formato PDF ou HTML;

1.9.32. Possibilitar rotação do log;

1.9.33. Suportar geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

1.9.33.1. Resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda;

1.9.33.2. Principais aplicações por taxa de transferência de bytes,

1.9.33.3. Principais hosts por número de ameaças identificadas;

1.9.33.4. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus, Antiphishing e Anti-Malware), de redes vinculadas a este tráfego;

1.9.34. Deve permitir a criação de relatórios personalizados;

1.9.35. O gerenciamento centralizado deverá ser entregue como appliance virtual e dever ser compatível/homologado com/para VMWare ESX (vSphere 5.1, 5.5 ou 6);

1.9.36. A solução de gerenciamento deve possui a capacidade de gerenciar outros Firewalls de segurança do mesmo fabricante mesmo estão em ambientes virtualizados e nuvens públicas (AWS e Azure) e nuvens privadas (VMWare NSX ou Cisco ACI);

1.9.37. Possui capacidade de integração com soluções de terceiros via API e também suportar configurações através de RestAPI;

1.9.38. Deve consolidar logs e relatórios de todos os dispositivos administrados;

1.9.39. Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;

1.9.40. Deverá possuir mecanismo de Drill-Down para navegação e análise dos logs em tempo real;

1.9.41. Nas opções de Drill-Down, deve ser possível identificar o usuário que fez determinado acesso;

1.9.42. Permitir que os relatórios possam ser salvos, enviados e impressos;

1.9.43. Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino, etc;

1.9.44. A solução deve prover, no mínimo, as seguintes funcionalidade para análise avançada dos incidentes:

1.9.45. Visualizar quantidade de tráfego utilizado de aplicações e navegação;

1.9.46. Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;

1.9.47. A solução de correlação deve possuir mecanismo para detectar login de administradores em horários irregulares;

1.9.48. A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

1.9.49. Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando para tanto gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos;

1.9.50. Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory via Radius;

1.9.51. Permitir criações de políticas de acesso de usuários autenticada no Active Directory, de forma que reconheça os usuários de forma transparente;

1.9.52. Geração de painel e relatórios contendo mapas geográficos gerados em tempo real para a visualização das principais ameaças através de origens e destinos do tráfego gerado na Instituição;

1.9.53. A plataforma de gerência centralizada e monitoração deve possibilitar a visualização dos logs de Firewall, navegação web, conteúdo de arquivos, prevenção de ameaças e Sandbox, todos a partir de um único local centralizado possibilitando a procura correlacionada de logs em uma única tela, como, por exemplo, pesquisar logs de Antivírus e navegação web simultaneamente na mesma query de pesquisa.

1.9.54. O relatório das emulações (sandboxing) deve conter de maneira detalhada as atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado;

1.9.55. Possuir mecanismo para que logs antigos sejam removidos automaticamente;

1.9.56. Possuir a capacidade de personalização de gráficos como barra, linha e tabela;

1.9.57. Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;

1.9.58. Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU;

1.9.59. A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências;

1.10. Capacitação Técnica

1.10.1. O treinamento deverá ser completo para contemplar a instalação, customização, operação e administração da solução de firewall para 5 (cinco) funcionários da CONTRATANTE, na modalidade de Ensino a Distância (EAD), online e ao vivo;

1.10.2. O treinamento deverá ser ministrado para turma especifica para a CONTRATANTE;

1.10.3. Serão aceitos cursos oficiais do fabricante da solução;

1.10.4. Deverá possuir módulos teóricos e práticos;

1.10.5. Os instrutores devem ser certificados pelo fabricante da solução para o treinamento;

1.10.6. O conteúdo dos cursos deverá abranger, minimamente, os seguintes tópicos:

1.10.6.1. Configuração – acesso e navegação na solução; comando de configurações básicas e avançadas; estrutura/arquitetura do sistema operacional dos equipamentos; configuração via CLI, GUI, Client e web;

1.10.6.2. Operação – comandos de gerenciamento e monitoramento da saúde dos recursos dos equipamentos; aplicação de bloqueios manuais e automáticos e criação de filtros;

1.10.7. Ao final do treinamento deve ser emitido certificado de conclusão para cada participante/aluno constando a carga horária e a ementa.

1.11. Instalação e configuração

1.11.1. Os serviços de instalação e configuração deverão ser executados por técnico(s) certificado(s) pelo fabricante;

1.11.2. Os serviços de instalação compreendem as atividades de planejamento, instalação física, instalação lógica e finalização da solução no ambiente da CONTRATADA.

1.11.3. Os serviços de configuração consistem em ajustar todos os parâmetros necessários (físicos e lógicos) para o funcionamento da solução e a sua adequação para funcionamento no ambiente da CONTRATADA atendendo aos requisitos dessa especificação;

1.11.4. Caberá à CONTRATADA todo o processo de planejamento, a instalação, a configuração, a integração, os testes e a compatibilidade dos equipamentos, que deverão ser integrados à infraestrutura de Tecnologia de Informação existente no local de instalação dos equipamentos;

1.11.5. A instalação compreenderá a migração das configurações e regras existentes no ambiente atual do CONTRATANTE, suportado por um cluster de firewalls checkpoint , assim como as demais configurações de segurança e disponibilidade.

1.12. Operação Assistida

1.12.1. A operação assistida deverá ocorrer durante 45 dias corridos a partir da instalação e configuração da solução na CONTRATANTE;

1.12.2. O serviço de operação assistida é composto por um conjunto de atividades que permitem o treinamento e a capacitação da equipe da CONTRATANTE responsável pelas atividades de operação, manutenção preventiva e corretiva, transferindo todo o conhecimento e experiência necessária para a operação da solução;

1.12.3. Durante os 45 dias corridos, será prestado todo o suporte necessário para a operacionalidade da solução, minimizando o risco da implantação da solução e proporcionando as condições ideais para transferência da tecnologia envolvida em regime de treinamento enquanto trabalha, até que a CONTRATANTE possa assumir as atividades com sua própria equipe;

1.12.4. Durante a operação assistida também será necessário realizar, pela CONTRADADA, possíveis customizações e ajustes finais que forem identificados durante o período de instalação, configuração e operação assistida;

1.12.5. Por padrão, a prestação da operação assistida ocorrerá presencialmente nas dependências da CONTRATANTE ou remotamente a ser definido pela CONTRATANTE;

1.12.6. A CONTRATADA deverá fornecer suporte técnico especializado em formato de Banco de horas para a solução ofertada;

1.12.7. A CONTRATADA deverá realizar a prestação de serviço remoto no modelo de banco de horas com um total de 300h, observando-se o consumo máximo de 16h/mês para ser utilizado durante a vigência do contrato e com pagamento somente se forem utilizadas.

1.13. Suporte, manutenção e atualização de versão

1.13.1. O suporte técnico compreende o diagnóstico e identificação de problemas, apoio técnico na utilização, correção de erros, defeitos (bugs) ou mau funcionamento sobre qualquer funcionalidade, recurso, componente ou módulo disponível de forma nativa na solução de firewall, ou decorrente de qualquer adaptação (customização) e ajuste (tuning) efetuada pela CONTRATANTE;

1.13.2. O atendimento a um chamado de suporte deverá ocorrer por qualquer uma das seguintes formas: contato telefônico, envio de mensagem eletrônica (e-mail), acesso ao sítio (website) da CONTRATADA ou do fabricante da solução de firewall, com controle de acesso por senha;

1.13.3. O atendimento telefônico sempre que aplicável e viável, por meio de ligação local em Belo Horizonte/MG ou ligação interurbana gratuita (0800);

1.13.4. A CONTRATANTE poderá efetuar um número ilimitado de chamados técnicos para a CONTRATADA, por qualquer uma das formas disponíveis, durante vigência do contrato vinculado a este edital;

1.13.5. Na abertura ou registro de um chamado técnico, por qualquer uma das formas disponíveis, a CONTRATADA deverá informar: data e hora de abertura do chamado, descrição do chamado, nível de severidade do chamado e identificação completa do solicitante;

1.13.6. A CONTRATADA deverá retornar, via e-mail, a confirmação da abertura do chamado técnico, doravante denominado confirmação do chamado, contemplando as seguintes informações na sua abertura: código de identificação do chamado, identificação do responsável da CONTRATADA pela abertura do chamado;

1.13.7. O atendimento ao chamado técnico pela CONTRATADA deverá ocorrer pelo menos por uma das seguintes formas: chamada telefônica, envio de mensagem eletrônica (e-mail), recursos disponíveis no sítio (site) do fabricante da solução de firewall ou da CONTRATADA, presencial ou suporte por acesso remoto;

1.13.8. Caso acionado o suporte direto do fabricante, este deverá ter atendimento em português. Caso contrário, a CONTRATADA deverá ser responsável por intermediar os contatos entre o fabricante e a CONTRATANTE;

1.13.9. Um chamado técnico somente será considerado contingenciado ou concluído com o aceite da CONTRATANTE, na forma de um visto na ordem de serviço correspondente ou aceite por e-mail ou ainda, diretamente no sistema oferecido pela CONTRATADA, caso esta forma seja utilizada;

1.13.10. Após apresentar uma solução de contorno para o chamado técnico, a CONTRATADA deverá retornar, via e-mail, a confirmação da execução do serviço, contemplando as seguintes informações: código de identificação do chamado, data e hora de conclusão do atendimento, descrição dos serviços executados e/ou da solução apresentada;

1.13.11. Em caso de adoção de solução de contorno, sem prejuízo da solução definitiva cabível, a CONTRATADA deverá emitir laudos, na periodicidade exigida pela CONTRATANTE, informando sobre a evolução dos trabalhos para solucionar o problema de forma definitiva;

1.13.12. Após apresentar uma solução definitiva para o CHAMADO TÉCNICO, a CONTRATADA deverá retornar, via e-mail, a confirmação da execução do serviço, contemplando as seguintes informações: código de identificação do chamado, data e hora de conclusão do atendimento, descrição dos serviços executados e/ou da solução apresentada;

1.13.13. Deverá ser garantido à CONTRATANTE o pleno acesso ao sítio (site) dos fabricantes dos produtos que compõem a solução de firewall, com direito a consultas a quaisquer bases de conhecimentos e fóruns de discussão disponíveis para seus usuários;

1.13.14. Caberá exclusivamente à CONTRATANTE a decisão de implantar ou não quaisquer atualizações de software fornecidos pela CONTRATADA;

1.13.15. A CONTRATADA deverá disponibilizar mecanismos para a atualização de software pelo download direto através da própria aplicação, pelo envio das mídias ou através de download no seu sítio (site) ou do fabricante do software em questão;

1.13.16. O serviço de manutenção consiste na correção de qualquer problema ou falha apresentados em componentes físicos ou lógicos da solução;

1.13.17. A atualização de software é uma alteração da versão anterior com o objetivo de implementar melhorias. Essas melhorias podem ser de usabilidade, correção de falhas, desempenho, adição de novas funcionalidades, etc.;

1.13.18. O prazo de atualização de todo software fornecido deve ser igual ao período de garantia do produto. Durante a vigência do contrato, a CONTRATANTE terá direito a todas atualizações de versão e release dos softwares.

1.14. Garantia

1.14.1. O(s) equipamento(s) que compõe(m) a solução devem estar em linha de fabricação até a data de assinatura do contrato e a data de final de suporte (end-of-support) deve ser após término do contrato desta solução;

1.14.2. O serviço de Garantia contempla garantir o correto e pleno funcionamento de todos os itens adquiridos, seja hardware, software e os componentes necessários para o funcionamento da solução;

1.14.3. A CONTRATADA deverá garantir a substituição de qualquer módulo defeituoso, incluindo hardware, software ou componentes necessários para o funcionamento da solução durante o prazo contratado; bem como o próprio equipamento se for necessário;

1.14.4. Não haverá custos adicionais para a CONTRATANTE de substituição de quaisquer componentes durante o período de garantia;

1.14.5. Prazo de garantia deverá ser de 60 meses.

2. LOTE 2. WEB APPLICATION FIREWALL APPLIANCE VIRTUAL

2.1. Características Gerais

2.1.1. Não serão aceitos produtos ou serviços do tipo demo, trial e open-source. A solução deve ser proprietária;

2.1.2. A solução de WAF deverá ser fornecida em appliance virtual;

2.1.3. O appliance virtual deverá ser compatível com VMWARE e KVM, além de estar disponível no marketplace da AWS, GCP e Azure para contratação no modelo Bring Your Own License (BYOL);

2.1.3.1. Caso não seja possível a instalação em ambiente *on premises*, o licenciamento poderá sere realizado em nuvem privada do fabricante desde que sem custos adicionais ao contratante.

2.1.4. A solução deve ser capaz de visualizar, via console, as informações de saúde e desempenho de todo o ambiente que a compõem, incluído softwares e equipamentos;

2.1.5. Possuir suporte a SNMP v2c e v3;

2.1.6. Enviar mensagens por e-mail e traps SNMP;

2.1.7. Os componentes da solução poderão ser executados num mesmo appliance, ou poderão ser distribuídos em múltiplos appliances, de acordo com a característica de cada produto, respeitadas as características de funcionamento e performance exigidas neste edital;

2.1.8. A solução deverá ter o pleno funcionamento independentemente de conexão (física ou lógica) com o fabricante, exceto para atualizações de versões e de segurança;

2.1.9. Suportar IPV6;

2.1.10. A solução deverá possuir a capacidade para suportar a adição de novos componentes (hardware e/ou software) escaláveis sem causar interrupções no funcionamento da solução;

2.1.11. Apresentar uma relação descritiva dos componentes fornecidos, incluindo seus códigos comerciais;

2.1.12. Não será aceito equipamento do tipo NGFW (Next Generation Firewall).

2.2. Características do Appliance

2.2.1. Deve ser capaz de executar todas as suas funções de aprendizado, análise e proteção de tráfego web considerando pelo menos uma taxa de transferência de 1 Gbps;

2.2.2. A solução deve ter vários mecanismos de implantação (deployment) com pelo menos uma ponte transparente na linha (Bridge L2), Proxy Reverso. Deve possuir a capacidade de monitorar e auditar todos os acessos de modo (passivo) a fim de monitorar o tráfego sem fazer alterações na rede;

2.2.3. A solução deve permitir a integração nos modos proxy reverso explícito e proxy reverso transparente (Bridge L2);

2.2.4. A solução deve ter um impacto de milissegundos na latência da rede;

2.2.5. O sistema deve permitir a integração e envio de alertas para terceiros ou ferramentas de correlação (SIEM). Será permitido que a integração seja realizada através da exportação de eventos utilizando SYSLOG ou através de RestAPI;

2.2.6. O equipamento deve suportar o protocolo de gerenciamento de rede SNMP a ser monitorado por ferramentas de terceiros;

2.2.7. Todos os componentes da solução de WAF com recursos para efetuar o balanceamento de carga entre aplicações devem ser do mesmo fabricante dos appliances, ou serem homologados pelo mesmo, ou compatíveis com outros fabricantes, podendo a CONTRATANTE realizar diligência junto ao mesmo para esta comprovação quando da recepção técnica da solução. As funcionalidades de WAF e balanceamento de carga entre aplicações web do TRF6 podem ser ofertadas no mesmo applicance ou em appliances distintos;

2.2.8. A solução de WAF com balanceamento de carga entre aplicações Web ofertada de maneira integrada deve ser composta de no mínimo um cluster com dois applicances;

2.2.9. Caso a solução de WAF seja ofertada separadamente da solução balanceamento de carga entre aplicações Web, tanto a solução de WAF quanto a solução de balanceamento deve ser composta de no mínimo um cluster com dois applicances ou servidores cada;

2.2.10. A solução de WAF e a solução de balanceamento entre aplicações web devem ser do mesmo fabricante;

2.2.11. A capacidade de processamento da solução deverá seguir as melhores práticas de cada fabricante, considerando todos os requisitos de capacidade definidos nesta especificação, tais como: trafego, conectividade, conexões, requisições nível 7, requisições SSL, transações e compressão;

2.2.12. Deve possuir CPU e memória suficientes para atender aos throughputs definidos no edital tanto para WAF quanto para o balanceador sem degradação de performance da solução quando ativada simultaneamente as duas funcionalidades;

2.2.13. Os equipamentos que serão responsáveis pela inspeção de tráfego web e pelo balanceamento de carga para soluções ofertadas em appliances distintos, deverão suportar, cada um de forma independente, o throughput de pelo menos 1 (um) Gbps tanto para a funcionalidade de firewall de aplicação Web como para a funcionalidade de balanceamento de carga entre aplicações;

2.2.14. As soluções de WAF com balanceamento ofertadas no mesmo appliance deverão suportar o throughput de pelo menos 1 (um) Gbps em cada appliance do cluster.

2.3. Balanceamento, Cache e Aceleração Web

2.3.1. Deve suportar no mínimo 1 Gbps (um Gigabits por segundo) de inspeção de tráfego na camada 7. Para alcançar esse throughput será aceito que o equipamento faça cache, em memória RAM ou SSD, do conteúdo estático, como por exemplo imagens, após a sua primeira inspeção. Todo conteúdo estático permitido em cache não será reinspecionado até a expiração do cache;

2.3.2. A solução fornecida deverá operar em cluster oferecendo alta disponibilidade com tolerância a falhas, independentemente da quantidade de elementos que compõe o cluster;

2.3.3. Na falha de um dos elementos do cluster, não poderá haver nenhuma degradação ou indisponibilidade das aplicações;

2.3.4. Deve suportar configuração de mTLS em um virtual server de aplicação do TRF6;

2.3.5. Deve suportar configuração de mTLS por url e path de aplicação do TRF6;

2.3.6. A solução deve ser capaz de trabalhar com recursos de alta disponibilidade, permitindo a ligação de dois ou mais equipamentos possibilitando configurar um único IP dos recursos protegidos nos dois ou mais equipamentos;

2.3.7. Deve ser fornecido todos os recursos possíveis de redundância sem nenhuma despesa com licenças adicionais;

2.3.8. A solução deve permitir a configuração das interfaces de alta disponibilidade do cluster (heartbeat), com opções para:

2.3.8.1. Compartilhar a rede de heartbeat com a rede de dados;

2.3.8.2. Utilizar uma rede exclusiva para o heartbeat.

2.3.9. A solução deverá ser capaz de trabalhar no modo Ativo/Standby, com equipamento de mesmo fabricante;

2.3.10. A solução deverá ser capaz de trabalhar no modo Ativo/Ativo, mantendo o status das conexões;

2.3.11. Aceita-se como Ativo-Ativo a utilização de dois endereços Virtuais, onde cada endereço fica ativo em um elemento e em espera no outro;

2.3.12. A solução deve suportar múltiplas tabelas de rotas independentes;

2.3.13. O equipamento, quando habilitado para mais de uma função (Server Load Balancing (SLB), Aceleração Web, etc.), deverá permitir a definição da importância da função, determinando quantidade de processamento (CPU e memória) serão alocados para cada tipo de funcionalidade;

2.3.14. A solução deve possuir capacidade para gerenciar os recursos disponíveis de acordo com as funções habilitadas nos equipamentos SLB, GSLB, aceleração Web, etc.;

2.3.15. A solução deverá suportar e estar licenciado para todas as aplicações comuns de um Switch Layer 7 (sete):

2.3.15.1. Server Load-Balancing;

2.3.15.2. Firewall Load-Balancing;

2.3.15.3. Proxy Load-Balancing;

2.3.16. A solução deverá possuir recursos para balancear servidores do TRF6 com qualquer hardware, sistema operacional e tipo de aplicação;

2.3.17. Suportar Balanceamento apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;

2.3.18. A solução deve permitir o encapsulamento, em camada 3, do tráfego entre o balanceador e o servidor para tráfego IPv4 e IPv6, quando o balanceamento é realizado apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;

2.3.19. A solução deve ser capaz de abrir um número reduzido de conexões TCP com o servidor e inserir os HTTP requests gerado pelos clientes nestas conexões, reduzindo a necessidade de estabelecimento de conexões nos servidores e aumentando a performance do serviço;

2.3.20. A solução deve suportar e estar licenciado para os seguintes métodos de balanceamento para as aplicações do TRF6:

2.3.20.1. Round Robin;

2.3.20.2. Least Connections;

2.3.20.3. Weighted Percentage (por peso);

2.3.20.4. Servidor ou equipamento com resposta mais rápida baseado no tráfego real;

2.3.21. Weighted Percentage dinâmico (baseado no número de conexões);

2.3.22. Dinâmico, baseado em parâmetros de um determinado servidor ou equipamento, coletados via SNMP ou WMI;

2.3.23. A solução deve ser capaz de balancear as novas sessões, preservando as sessões existentes no mesmo servidor e implementando persistência de sessão dos seguintes tipos:

2.3.23.1. Por cookie – inserção de um novo cookie na sessão;

2.3.23.2. Por cookie – utilização do valor do cookie da aplicação, sem adição de cookie;

2.3.23.3. Por endereço IP destino;

2.3.23.4. Por Endereço IP origem;

2.3.23.5. Por sessão SSL;

2.3.23.6. Através da análise da URL acessada;

2.3.23.7. Através da análise de qualquer parâmetro no header HTTP;

2.3.23.8. Através da análise de qualquer informação da porção de dados (camada 7);

2.3.24. A solução deve utilizar Cache Array Routing Protocol (CARP) no algoritmo de HASH ou utilizando algum protocolo ou solução similar;

2.3.25. A solução deverá suportar os seguintes métodos de monitoramento dos servidores reais:

2.3.25.1. Layer 3 – ICMP;

2.3.25.2. Conexões TCP e UDP pela respectiva porta no servidor;

2.3.26. Devem existir monitores predefinidos para, no mínimo, os seguintes protocolos: ICMP, HTTP, HTTPS, FTP, SMB, RADIUS, NNTP, RPC, LDAP, IMAP, SMTP, POP3, SIP, SOAP, SNMP. Caso não exista um monitor pré-definido deve ser possível criar um monitor de forma manual;

2.3.27. A solução deverá possuir recursos para limitar o número de sessões estabelecidas com cada servidor fisico;

2.3.28. A solução deverá possuir recursos para limitar o número de sessões estabelecidas com cada servidor virtual;

2.3.29. A solução deverá possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores;

2.3.30. A solução deve possuir as seguintes funcionalidades de segurança ativas e licenciadas:

2.3.30.1. Network Address Translation (NAT);

2.3.30.2. Proteção contra Denial of Service (DoS);

2.3.30.3. Proteção contra Syn flood;

2.3.30.4. Implementar Listas de Controle de Acesso (ACL);

2.3.30.5. Permitir o controle da resposta ICMP por servidor virtual;

2.3.30.6. Realizar Limpeza de cabeçalho HTTP;

2.3.30.7. Análise em Camada 7 de Protocolos, com alertas para violações na camada de Protocolo HTTP.

2.3.31. Possuir recursos para executar compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;

2.3.32. Deve ser possível definir qual tipo de compressão será habilitada (gzip1 a gzip9, deflate);

2.3.33. Deve ser possível definir compressão especificamente para certos tipos de objetos;

2.3.34. A solução deve possuir recursos para fazer aceleração de SSL, onde os certificados digitais são instalados no equipamento e as requisições HTTP são enviadas aos servidores sem criptografia;

2.3.35. A solução deve ser capaz de ser configurada para recriptografar em SSL a requisição ao enviar para o servidor, permitindo as demais otimizações em ambiente 100% criptografado;

2.3.36. Suportar a utilização de memória RAM como cache de objetos HTTP, para responder às requisições dos usuários sem utilizar recursos dos servidores;

2.3.37. Possuir capacidade, no uso do recurso de cache, em definir quais tipos de objeto serão armazenados em cache e quais nunca devem ser cacheados;

2.3.38. Garantir que o recurso de cache possa ajustado em relação a quantidade de memória que será utilizada para armazenar objetos;

2.3.39. Possuir a capacidade para determinar qual o tamanho máximo do objeto a ser cacheado;

2.3.40. Possuir a capacidade para determinar qual o tamanho do menor objeto a ser cacheado;

2.3.41. Possuir a capacidade para determinar a URI (Uniform Resource Identifiers) que deve ser cacheada;

2.3.42. Possuir a capacidade para ler, alterar e ignorar o parâmetro cache-control no cabeçalho HTTP;

2.3.43. Possuir a capacidade para inserir e alterar o parâmetro age header no cabeçalho HTTP;

2.3.44. Suporte a otimização do protocolo TCP para ajustes a parâmetros das conexões clientes e servidor;

2.3.45. A solução deve suportar Internet Content Adaptation Protocol (ICAP);

2.3.46. Deve ser capaz de realizar DHCP relay;

2.3.47. A Solução deve ter a capacidade de permitir a criação de MIBs customizadas;

2.3.48. A Solução deve ter suporte a sFlow;

2.3.49. A solução deve ter suporte a, no mínimo, TLS 1.2, SHA 2 Cipher e SHA256 hash;

2.3.50. A solução deve ser capaz de colocar em fila as requisições TCP que excedam a capacidade de conexões do grupo de servidores ou de um servidor. O balanceador não deverá descartar as conexões que excedam o número de conexões do servidor ou do grupo de servidores;

2.3.51. Deve ser possível configurar o tamanho máximo da fila;

2.3.52. Deve ser possível configurar o tempo máximo de permanência na fila;

2.3.53. A solução deve realizar Controle de Banda Estático para grupos de aplicações e rede;

2.3.54. A solução deve realizar Controle de Banda Dinâmico para grupos de aplicações e rede;

2.3.55. A solução deve realizar Controle de Banda baseado em domínio de roteamento;

2.3.56. A solução deve possuir suporte ao espelhamento de conexões FTP, Telnet, HTTP, UDP, SSL;

2.3.57. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra-ataques;

2.3.58. Permitir a criação de políticas através de interface gráfica web para manipulação de tráfego através de lógica para pelo menos os seguintes operadores: GEOIP, http-basic-auth, http-cookie, http-header, httphost, http-method, http-referer, http-set-cookie, http-status, http-uri e http-version;

2.3.59. Deve ser possível tomar as seguintes ações através dessas políticas:

2.3.59.1. Bloqueio de tráfego;

2.3.59.2. Reescrita e manipulação de URL;

2.3.59.3. Registro de tráfego (log);

2.3.59.4. Adição de informação no cabeçalho HTTP;

2.3.59.5. Redirecionamento do tráfego para um membro específico;

2.3.59.6. Selecionar uma política específica para Aplicação Web.

2.3.59.7. Deverá possuir inteligência artificial para detecção além das assinaturas pré-definidas.

2.4. Características de Proteção de Aplicações Web

2.4.1. A solução pode executar automaticamente varreduras de rede que permitem a descoberta de novos servidores e serviços nos protocolos HTTP e HTTPS;

2.4.2. A solução deve proteger a infraestrutura web das aplicações de ataques contra a camada de aplicação (Camada 7);

2.4.3. A solução deve fornecer a possibilidade de bloquear transações WEB de maneira preventiva, antes que elas cheguem via rede ao servidor;

2.4.4. Deve ser capaz de correlacionar eventos ou violações de políticas;

2.4.5. A solução deve detectar, alertar e bloquear opcionalmente, em tempo real, qualquer comportamento malicioso conhecido e/ou desconhecido;

2.4.6. A solução deve ter um modo de aprendizado que permita definir quais ações são esperadas e aceitas pelos usuários;

2.4.7. No modo de aprendizado, o sistema deve aprender a estrutura e os elementos do aplicativo e essas informações devem estar disponíveis para automatizar a configuração do modelo de segurança positivo. Pelo menos você deve aprender sobre: Hosts válidos, URLs, parâmetros, cookies, tipo de conteúdo dos parâmetros;

2.4.8. No modo de aprendizado, deve aprender além do comportamento esperado do usuário e essas informações devem estar disponíveis para automatizar a configuração do modelo de segurança positivo. No mínimo, você deve aprender sobre: Caracteres aceitos, tamanho do valor esperado;

2.4.9. O modo de aprendizagem pode ser ativado e desativado manualmente para estender o tempo de reconhecimento do padrão de comportamento;

2.4.10. O modo de aprendizagem deve poder permanecer ativo mesmo quando está em modo de proteção ou bloqueio, permitindo a incorporação de novos parâmetros ou características do mesmo sem ter que fazê-lo manualmente. De tal forma que a configuração de segurança positiva é atualizada automaticamente e constantemente;

2.4.11. Com relação a quaisquer ataques ou outra atividade não autorizada, a solução deve ser capaz de tomar as medidas adequadas, pelo menos: Terminar solicitações e respostas, bloquear a sessão TCP, isolados em quarentena temporária ou bloquear o usuário do aplicativo, colocar em quarentena temporária ou bloquear o endereço IP de origem;

2.4.12. A solução deve ter um conjunto de padrões correspondentes aos ataques conhecidos. Esta base de dados de padrões deve poder ser atualizada periodicamente, automaticamente e sem ajuda;

2.4.13. A solução deve permitir a definição para as regras e alarmes, condições lógicas em que o alarme ou o bloqueio não sejam ativos se não aconteceu o evento, pelo menos, um número de vezes definido dentro de um período de tempo definido e associado a um contexto de conexão definível;

2.4.14. A solução deve ter a capacidade de proteger os serviços Web com base no SOAP;

2.4.15. A solução deve ter a capacidade de receber e usar certificados e pares de chaves pública / privada para servidores da Web protegidos;

2.4.16. A solução deve poder inspecionar e monitorar todos os dados HTTP/S do aplicativo, incluindo cabeçalhos HTTP, campos de formulário e o corpo de solicitações HTTP/S;

2.4.17. A solução deve inspecionar as solicitações e as respostas HTTP/S;

2.4.18. A solução deve ser capaz de validar todos os tipos de dados inseridos, incluindo URLs, formulários, cookies, consultas, campos e parâmetros ocultos, métodos HTTP, elementos XML e ações SOAP;

2.4.19. A solução deve ser capaz de identificar o usuário do aplicativo da Web. A identificação deve persistir até que o usuário tenha deixado o aplicativo;

2.4.20. A solução deve ser capaz de identificar e manter um registro das sessões da Web no nível do aplicativo, por meio de cookies de rastreamento ou parâmetros do aplicativo;

2.4.21. A solução deve ser capaz de aplicar uma correção virtual (virtual patching) para proteger as vulnerabilidades detectadas e deve ter integração com scanners de vulnerabilidade (pelo menos 3 soluções ou serviços diferentes do mercado) para receber os seus resultados ou relatórios, interpretar e sugerir mudanças para aplicar como correção virtual;

2.4.22. A solução deve suportar a detecção de ferramentas de download automático, bots, scripts, etc. através da geração de um requisito em JavaScript, a fim de bloquear todas as consultas que não possuem um navegador real por trás;

2.4.23. A solução deve ser capaz de implementar controles anti-scrapping de forma nativa, permitindo bloquear tentativas automatizadas de roubar informações do site;

2.4.24. A solução deve ser capaz de reconhecer IPs de fontes mal-intencionadas (como redes TOR, proxies anônimos, sites de Phishing, etc.) e também ter catalogação de IPs por geolocalização. Essas informações devem ser atualizadas periodicamente e deve ser possível integrar políticas de segurança como um critério;

2.4.25. Ser capaz de diferenciar entre as requisições legítimas realizadas por usuários humanos das requisições realizadas por bots, web scraping e ataques automatizados;

2.4.26. A solução deve fornecer proteção automatizada para todas as vulnerabilidades expressas no OWASP Top 10;

2.4.27. A solução deve permitir a geração de exceções para as políticas de segurança de validação de protocolo por URL ou IP de origem;

2.4.28. A solução deve permitir a inspeção das conexões SSL (SSL v3, TLS v1) implementadas nos servidores da web. Para isso, os certificados (chave pública e privada) podem ser importados;

2.4.29. A solução deve validar se o conteúdo e a duração do protocolo HTTP, incluindo os cabeçalhos, corpo e cookies, estão corretos. Por sua vez, você deve ser capaz de restringir os métodos HTTP usados em um aplicativo da Web (GET, POST, PUT, etc.);

2.4.30. A solução deve permitir ações e alertar para violações de protocolos inferiores ao aplicativo, incluindo inspeção de pacotes IP, TCP, UDP e seus cabeçalhos;

2.4.31. A solução deve proteger os aplicativos da Web contra ataques comuns, como:

- 2.4.31.1. Injeção SQL (SQL Injection);
- 2.4.31.2. Injeção de LDAP (LDAP Injection);
- 2.4.31.3. Comando do SO (SO Commanding);
- 2.4.31.4. Injeção SSI (SSI Injection);
- 2.4.31.5. Inclusão remota de arquivos (Remote File Inclusion);
- 2.4.31.6. Mail Command Injection;
- 2.4.31.7. Injeção de XML (XML Injection);
- 2.4.31.8. Injeção Xpath (XPath Injection);
- 2.4.31.9. Injeção Xquery (XQuery Injection);
- 2.4.31.10. Cross Site Scripting (XSS);
- 2.4.31.11. Cross Web Request Forgery (CSRF);
- 2.4.31.12. Web Scrapping;
- 2.4.31.13. Navegação forçada (Forceful Browsing).

2.4.32. Proteção de modificação de campos ocultos;

2.4.33. Permite a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;

2.4.34. A solução deve suportar a definição de políticas diferentes que podem ser associadas a cada aplicativo individualmente;

2.4.35. Para cada aplicação protegida, o administrador deve ser capaz de configurar em que momento é feita a detecção (log) dos ataques recebidos e quando eles evitam (bloqueiam) os ataques;

2.4.36. Para cada aplicativo da Web, deve ser possível desabilitar a prevenção de ataques (bloqueio) e deixar apenas a detecção (log) em formato granular para facilitar a solução de problemas por tipos de ataques;

2.4.37. No caso de um bloqueio, dependendo do modo de operação, a resposta (página) enviada ao usuário deve poder ser personalizada;

2.4.38. A solução deve permitir que hosts ou clientes confiáveis sejam excluídos das medidas de proteção;

2.4.39. A solução deve suportar a identificação do IP de origem no caso de passar por proxy, interpretando o campo X-forwarded-for do cabeçalho HTTP;

2.4.40. A solução deve validar se o conteúdo e a duração do protocolo HTTP, incluindo os cabeçalhos, corpo e cookies, estão corretos;

2.4.41. Deve possuir hardware dedicado para inspeção otimizada de tráfego criptografado com SSL e TLS;

2.4.42. A latência inserida no tráfego SSL não pode superar os 5ms (cinco milissegundos);

2.4.43. A solução deve suportar o uso de firewall camada 3 e 4 junto com firewall camada 7 no mesmo appliance para evitar problemas com o aumento da latência;

2.4.44. A solução deve suportar responder por 1 endereço IP e vários endereços IPs por aplicação web;

2.4.45. Deve poder atuar como Web Application Firewall em modo WAF Positivo (permitindo apenas o que é conhecido e esperado);

2.4.46. Deve poder atuar como Web Application Firewall em modo WAF Negativo (bloqueando características conhecidas de ataque);

2.4.47. Deve ser capaz de operar usando modelo positivo de segurança, por meio de aprendizado e de definição de regras que descrevem o comportamento esperado de um aplicativo ou serviço, efetuando o bloqueio de todo o tráfego que não coincide com essas regras (árvore de acesso válido);

2.4.48. Possuir as seguintes características:

2.4.48.1. Facilidade para liberação de regras aprendidas automaticamente que estejam gerando grande quantidade de falso positivo;

2.4.48.2. Facilidade para transformar um ataque detectado e considerado falso positivo como regra do firewall;

2.4.48.3. Facilidade para aplicar diferentes regras para diversas aplicações;

2.4.48.4. Capacidade para customizar regras de negação de serviço;

2.4.48.5. Capacidade para combinar detecção e prevenção na construção das regras;

2.4.48.6. Capacidade para desfazer a aplicação de uma regra.

2.4.49. Deve suportar o modelo de segurança positivo, devendo ser capaz de aprender qual perfil de tráfego é legítimo e bloquear ataques ou atividades não autorizadas;

2.4.50. Deve possuir políticas de segurança de aplicações web pré-configuradas na solução;

2.4.51. Deve permitir a criação de políticas diferenciadas por aplicação;

2.4.52. Deve possuir funcionalidade que ajuste dinamicamente o nível de proteção na detecção de ataques;

2.4.53. Deve ser possível utilizar uma política em múltiplas aplicações (uma para várias);

2.4.54. Deve ser possível utilizar uma política para cada aplicação (uma para uma);

2.4.55. Deverá possuir funcionalidade de criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real observado à aplicação;

2.4.56. O perfil aplicação aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;

2.4.57. Deve identificar e criar um perfil de utilização das aplicações, mesmo que as páginas Web e conteúdos sejam dinâmicos, como os desenvolvidos em JavaScript, CGI, ASP, PHP e Java;

2.4.58. Deve suportar WebSocket Traffic Filter;

2.4.59. Deve suportar o controle de política granular baseada no caminho do aplicativo (application path);

2.4.60. Deve permitir a aceitação de falsos positivos (exceção à política de segurança);

2.4.61. Deve permitir que ao detectar um falso positivo, o administrador aceite a requisição e atualize a política automaticamente;

2.4.62. Deve suportar a configuração de hosts confiáveis para permitir a execução de operações não permitidas pela política adotada para uso em eventos de testes de penetração, solução de problemas (troubleshooting) e análise de performance;

2.4.63. Deverá possuir proteção baseada em assinaturas para prover proteção contra-ataques conhecidos;

2.4.64. Deverá ser possível desabilitar algumas assinaturas específicas em determinados parâmetros, como uma exceção à regra geral;

2.4.65. As atualizações de assinaturas deverão passar por um período configurável de testes, onde nenhuma requisição que viole a assinatura será bloqueada, apenas informada no relatório. Este processo deve ser automatizado, não sendo necessário criar regras específicas a cada atualização de assinatura;

2.4.66. A solução deverá realizar bloqueios de ataques mesmo sem assinaturas atualizadas;

2.4.67. Deverá implementar consultas a bases de reputação externas;

2.4.68. A solução deve ser capaz de decifrar tráfego SSL a partir da importação de chaves criptográficas, para permitir a inspeção de todo conteúdo do pacote originalmente cifrado;

2.4.69. Inspeção de tráfego através da troca de chaves assimétricas entre cliente e WAF (proxy SSL);

2.4.70. A solução deve suportar SSL Offload de conexões;

2.4.71. A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação. Essa inspeção poderá ser feita via integração ICAP;

2.4.72. A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação;

2.4.73. Permitir a integração com Firewall de Database de outros fabricantes;

2.4.74. Deve possuir tecnologia de detecção de anomalias baseado nos IDs dos dispositivos, permitindo a detecção de DoS, ataques de força bruta e ataques de sequestro de sessão. Deve ser possível filtrar relatórios por IDs de dispositivos;

2.4.75. A solução deverá permitir proteção contra envio de arquivos, considerando tamanho e tipo;

2.4.76. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar e aumentar a proteção contra-ataques recentes;

2.4.77. A solução deve se integrar com outras soluções de segurança como firewall, IPS e análise de logs de outros fabricantes;

2.4.78. Deverá armazenar os logs localmente ou exportar para Syslog server;

2.4.79. Possuir registro de logs com as seguintes características:

2.4.79.1. Em cada registro de log de acesso deve ser inserido um identificador de transação HTTP que deve ser único, envolvendo o par requisição/resposta;

2.4.79.2. Os registros de log de acesso e eventos devem ser armazenados em arquivo ou em banco de dados que permita a exportação ou em outro formato aberto como CSV ou TXT, podendo ainda serem armazenados localmente ou carregados (upload) em servidor de log via FTP ou SCP ou armazenados em servidor externo de banco de dados;

2.4.79.3. Permitir configurar a retenção dos logs por tempo e volume;

2.4.79.4. Ter capacidade para detecção, remoção ou codificação de dados sensíveis do log.

2.4.80. Deverá ser capaz de diferenciar acessos entre bots, Web scraping e usuários humanos para bloquear ataques automatizados;

2.4.81. Deve oferecer um serviço baseado na reputação do endereço IP de origem, protegendo as aplicações de serem acessadas pelas seguintes origens: Rede TOR, proxies anônimos e endereços IP de baixa reputação;

2.4.82. A Solução de Firewall de Aplicação deve suportar diferentes métodos de autenticação dos usuários das aplicações como: HTML Form, HTTP Basic Authentication, JSON/AJAX Request, NTLM, certificados SSL Client e HTTP Digest Authentication;

2.4.83. A solução deverá ser capaz de identificar e bloquear ataques através de:

2.4.83.1. Assinaturas, com atualização periódica da base pelo fabricante;

2.4.83.2. Regras de verificação personalizadas – política de segurança configurada;

2.4.83.3. Comportamento malicioso.

2.4.84. Deverá trabalhar com filtros de segurança:

2.4.84.1. De controle dos parâmetros das aplicações;

2.4.84.2. De proteção a sessão;

2.4.84.3. De controle de vulnerabilidades;

2.4.84.4. De controle de serviços Web;

6.2.4.84.5. De proteção a XML.

2.4.85. Permitir o bloqueio de ataques DoS/DDoS na camada 7, possuindo também a opção de apenas registrar o ataque, sem tomar nenhuma ação de bloqueio;

2.4.86. Não deve haver a necessidade de intervenção de usuário para configurar thresholds DoS pois esses valores devem ser autoajustáveis e adaptáveis de acordo com mudanças;

2.4.87. Possuir as seguintes formas de detecção de ataques DoS/DDoS na camada de aplicação:

2.4.87.1. Número de requisições por segundo enviados a uma URL específica;

2.4.87.2. Número de requisições por segundo enviados de um IP específico;

2.4.87.3. Detecção através de código executado no cliente com o objetivo de detectar interação humana ou comportamento de robôs (bots);

2.4.87.4. Número máximo de transações por segundo (TPS) de um determinado IP;

2.4.87.5. Aumento de um determinado percentual do número de transações por segundo (TPS);

2.4.87.6. Aumento do tempo de resposta (latência de aplicação) de uma determinada URL.

2.4.88. Deve permitir criar lista de exceção (whitelist) por endereço IP específico ou faixa de sub-rede;

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

2.4.90. Deverá permitir limitar o número de conexões e requisições por IP de origem para cada endereço IP Virtual;

2.4.91. Deve permitir adicionar, automaticamente e manualmente, em uma lista de bloqueio, os endereços IP de origem que ultrapassarem o limite estabelecido, por um período de tempo determinado através de configuração;

2.4.92. Permitir o bloqueio de determinados endereços IPs que ultrapassarem um número máximo de violações por minuto. O período de bloqueio deverá ser configurável e durante este período todas as requisições do cliente serão bloqueadas automaticamente;

2.4.93. A solução deve permitir o cadastro de robôs que podem acessar a aplicação;

2.4.94. Deve permitir o bloqueio de robôs (bots) que acessam a aplicação através de detecção automática, não dependendo de cadastros manuais;

2.4.95. Deve possuir mecanismo capaz de diferenciar entre bots e usuários humanos para bloquear ataques automatizados (robôs):

2.4.95.1. O mecanismo deve implementar mecanismos de desafios de Cookies, JavaScript e Captcha para reforçar a identificação de robôs;

2.4.95.2. O mecanismo deve consultar base de dados de robôs já conhecidos; 4.108.3 O mecanismo deve permitir a integração com o sistema de Captcha do Google.

2.4.96. Deverá permitir adoção de critérios de decisão para bloqueio e alerta, considerando no mínimo 7 (sete) critérios simultâneos, dentre eles:

2.4.96.1. Tempo de resposta de uma página web;

2.4.96.2. Tamanho da resposta de uma página web;

2.4.96.3. User-agent (navegador);

2.4.96.4. Usuário;

2.4.96.5. IP de origem

2.4.96.6. País de origem

2.4.96.7. Assinatura de ataque;

2.4.96.8. Conteúdo do payload;

2.4.96.9. Conteúdo do cabeçalho;

2.4.96.10. Conteúdo do cookie;

2.4.96.11. Código de resposta do servidor web;

2.4.96.12. Nome do host (Host Header);

2.4.96.13. Número de ocorrências num intervalo de tempo;

2.4.96.14. Método HTTP;

2.4.96.15. Horário.

2.4.97. Ao detectar um ataque ou qualquer atividade não autorizada, deve ser possível bloquear:

2.4.97.1. Requisições e respostas;

2.4.97.2. Uma conexão TCP;

2.4.97.3. Uma rede específica;

2.4.97.4. Um endereço IP durante um intervalo de tempo específico.

2.4.98. A solução deve fornecer, para cada política de segurança, múltiplas opções de evento posteriores ao bloqueio da requisição, dentre eles: Enviar log para Syslog Externo, enviar um e-mail, alerta para a interface de monitoração da gerência, executar um script definido pelo administrador e apresentar uma página de erro para o usuário;

2.4.99. Quando uma requisição for bloqueada pelo WAF, deve ser possível comunicar ao usuário sobre o fato através de uma página HTML informativa. 4.113 Deverá permitir a customização da resposta de bloqueio. Deve ser possível customizar a página HTML baseada em contextos como (Tipo de ataque, IP de Origem, Usuário e GeoLocalização) sendo configuradas através da GUI sem a necessidade de criação de scripts atém do HTML;

2.4.100. Deverá implementar proteção ao JSON (JavaScript Object Notation), REST (Representational State Transfer) e SOAP (Simple Object Access Protocol);

2.4.101. Deverá implementar proteção a API;

2.4.102. Deverá implementar proteção WebSockets;

2.4.103. Deverá implementar proteção sobre microsservicos;

2.4.104. Deve possuir suporte a filtro e validação de funções XML específicas da aplicação;

2.4.105. Prevenir o vazamento de informações, permitindo o bloqueio ou a remoção dos dados confidenciais;

2.4.106. Deve prevenir que erros de aplicação ou infraestrutura sejam mostrados ao usuário;

2.4.107. A solução deverá permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle;

2.4.108. A solução deverá ser capaz de interpretar o campo X-Forwarded-For como endereço IP de origem original de um pacote, a fim de identificar a origem real de tráfego que sofra NAT de origem;

2.4.109. Deverá proteger contra-ataques CSRF (Cross-Site Request Forgery), podendo ser possível especificar quais URLs serão examinadas;

2.4.110. A Solução deverá proteger, no mínimo, contra os ataques listados abaixo:

2.4.110.1. AJAX/JSON web threats;

2.4.110.2. Anonymous Proxy access

2.4.110.3. Application tampering;

2.4.110.4. Broken access control;

2.4.110.5. Buffer overflow;

2.4.110.6. Cross-site scripting (XSS);

2.4.110.7. Known Worms;

2.4.110.8. Malicious Encoding;

2.4.110.9. SQL injection;

2.4.110.10. Web Services (XML) attacks

2.4.110.11. XML bombs/DoS;

2.4.110.12. Brute force;

2.4.110.13. Cookie Injection;

2.4.110.14. Cookie manipulation;

2.4.110.15. Cookie poisoning;

2.4.110.16. Cross site request forgery (CSRF);

2.4.110.17. Directory Traversal;

2.4.110.18. Forceful browsing;

2.4.110.19. Hidden fields manipulation;

2.4.110.20. HTTP Denial of Service;

2.4.110.21. HTTP Response Splitting;

2.4.110.22. Illegal Encoding;

2.4.110.23. Layer 7 DoS and DDoS;

2.4.110.24. Malicious Robots;

2.4.110.25. OS Command Injection;

2.4.110.26. Parameter and HPP tampering;

2.4.110.27. Remote File Inclusion;

2.4.110.28. Request smuggling;

2.4.110.29. Sensitive data Exposure;

2.4.110.30. Session hijacking;

2.4.110.31. Web scraping;

2.4.110.32. Web server software and operating system attacks;

2.4.111. Deverá mitigar ataques de Slow HTTP;

2.4.112. A solução deve possuir lista dinâmica de endereços IP globais com atividades maliciosas;

2.4.113. A solução deve encriptar dados e credenciais na camada de aplicação, sem ter a necessidade de atualizar a aplicação;

2.4.114. Essas informações devem ser encriptadas para proteger o login e as credenciais dos usuários e com isso os dados da aplicação;

2.4.115. Deve ajudar a prevenir contra ataques de Credencial Stuffing, onde bases de credenciais expostas na Internet são usados para tentava de acesso de outras aplicações Web;

2.4.116. A solução deverá ser capaz de inspecionar e bloquear solicitações XML, SOAP e HTTP (versões HTTP 1.0, 1.1 e 2.0);

2.4.117. A solução deverá fazer checagem de:

2.4.117.1. Consistência de formulários;

2.4.117.2. Do cabeçalho do “user-agent” para identificar clientes inválidos; 4.131.3 Métodos HTTP utilizados (GET, POST, HEAD, OPTIONS, PUT, TRACE, DELETE, CONNECT), permitidos e bloqueados.

2.5. Gerenciamento

2.5.1. A solução deve ser gerenciada centralmente (configurações, controle e atualizações), através de interface web ou console de administração.

2.5.2. Possuir acesso controlado e autenticado por usuário, sendo que para a administração da solução deve-se usar uma conta para cada usuário administrador, independente da funcionalidade gerenciada.

2.5.3. O controle de acesso deve permitir a configuração de acesso por perfil às funções de Administração e Configuração de Regras.

2.5.4. Fornecer visualização e ações diferenciadas por perfis de acesso.

2.5.5. Permitir a visualização de painéis (dashboards).

2.5.6. Apresentar painéis gráficos (dashboards) com indicativos de situações diversas.

2.5.7. Deve possibilitar a CONTRATANTE, por meio do console de gerência, consultas sobre desempenho, problemas, configuração, mudanças e segurança do ambiente para cada domínio;

2.5.8. Deve armazenar as informações de desempenho do ambiente por um período mínimo de 30 (trinta) dias, mantendo estas informações disponíveis para a CONTRATANTE, sendo que o intervalo mínimo de coleta de informações dos elementos gerenciados deve ser de 05 (cinco) minutos, contendo no mínimo as seguintes informações:

2.5.8.1. Total de disponibilidade da Plataforma para um período mínimo 30 dias Por URL; Por conjunto de URL; Para todas as URL;

2.5.9. Deve possibilitar a geração de relatórios a qualquer tempo com as seguintes informações:

2.5.9.1. Total de GB (Gigabyte) consumido por domínio

2.5.9.2. Total de GB (Gigabyte) consumido no mês por todos os domínios;

2.5.9.3. Total de GB (Gigabyte) excedente, quando houver;

2.5.10. A solução deve permitir a emissão de relatórios gerenciais, conforme demanda da CONTRATANTE, com quantitativos e consumos por períodos;

2.5.11. A Plataforma deve possibilitar a consolidação de logs de toda a plataforma e seus recursos de forma global (todos os domínios) e individual (cada domínio) realizando seu armazenamento e retenção de forma segura;

2.5.12. Armazenar em log a identificação de tentativas de ataques e eventos gerados pela Plataforma e seus recursos, com no mínimo as seguintes informações:

2.5.12.1. Endereços IP que originaram os ataques;

2.5.12.2. Horário do ataque;

2.5.12.3. Nome do ataque;

2.5.12.4. Qual campo foi atacado;

2.5.12.5. Quantas vezes esse ataque foi realizado;

2.5.12.6. Técnicas utilizadas;

2.5.12.7. Eventos detectados que apontem:

2.5.12.8. Comportamentos maliciosos;

2.5.12.9. Comportamentos suspeitos;

2.5.12.10. Exploits;

2.5.12.11. Correlações de eventos;

2.5.12.12. Acessos;

2.5.13. Deve permitir, para toda a Plataforma e soluções que a compõem, a retenção de logs consolidados a cada 5(cinco) minutos por, no mínimo, 07(sete) dias;

2.5.14. Deve prover a retenção de logs detalhados por no mínimo 72 (setenta e duas) horas, para toda a Plataforma e soluções que a compõem;

2.5.15. Deve permitir que os logs sejam rotacionados de forma que os registros mais antigos sejam apagados quando não houver espaço de armazenamento disponível;

2.5.16. Deve possibilitar que por meio da console de gerência seja realizada a monitoração de logs e a investigação de logs;

2.5.17. Deve trabalhar com geolocalização para identificar a origem geográfica de um ataque;

2.5.18. Deve permitir exportar sob demanda os relatórios de logs em CSV;

2.5.19. Deve permitir o envio de logs para outros servidores de logs via syslog;

2.5.20. Deve permitir a configuração de alarmes personalizados, com base em investigações realizadas a partir dos logs;

2.5.21. Deve permitir apresentação dos dados consultados em vários formatos, incluindo tabela e gráficos;

2.5.22. Deve apresentar função de pesquisa por logs contendo no mínimo os seguintes critérios de pesquisa: Por dia, mês; Por domínio e endereço IP;

2.5.23. Deve permitir que sejam criados e aplicados filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, nome do ataque, o país de origem e destino;

2.5.24. Deve possibilitar a geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração; 5.25 Deve possibilitar a visualização do número de vezes que uma determinada regra foi usada (hits) em diferentes intervalos de tempo como dia, semana, mês ou intervalo customizável como data e horário de início e de fim da contagem; 5.26 Deve possibilitar a exportação de logs para fim de auditoria;

2.5.27. Possibilitar a exportação de logs para provedores de armazenamento compatíveis com S3;

2.5.28. Possibilitar a exportação de logs através de requisições HTTP para endpoints personalizados;

2.5.29. O equipamento deve fazer backup diário em forma automática de todas as informações nele armazenadas, incluindo as configurações de todos os módulos gerenciados e ter a capacidade de transferi-los automaticamente para um servidor remoto usando os protocolos SCP ou FTP;

2.5.30. Toda a configuração, administração e monitoramento da solução serão feitos através do console de administração;

2.5.31. A comunicação entre as estações de trabalho e o console de administração deve ser estabelecida através de um protocolo seguro com criptografia e autenticação por usuários locais, incluindo a possibilidade de usar certificados digitais;

2.5.32. A solução de administração deve permitir a atribuição de perfis de administração pelos usuários e esses perfis devem permitir a separação das funções de gerenciamento e monitoramento;

2.5.33. Capacidade de exportar logs para um formato SYSLOG ou SNMP TRAPS, para poder usar ferramentas de análise de terceiros;

2.5.34. O gerenciador deve possuir controle de interface gráfica Web (GUI: Graphical user interface) e interface por linha de comando (CLI – Command Line Interface);

2.5.35. A interface gráfica de gerenciamento deve ser cross-platform, em Web via protocolo HTTP e HTTPS, com suporte a acesso nativo via Microsoft Windows, Linux e Mac-OS;

2.5.36. Para interface gráfica do tipo Web, deve suportar no mínimo o navegador Mozilla Firefox e Chrome nas versões mais recentes;

2.5.37. A interface por linha de comando (CLI) deve possibilitar configuração dos equipamentos;

2.5.38. Deve possuir auto complementação de comandos;

2.5.39. Deve permitir acesso via SSH, criptografado;

2.5.40. Possuir um comando que mostre o tráfego de utilização das interfaces (bps e/ou pps);

2.5.41. Permitir reinicialização do equipamento;

2.5.42. Implementar Debugging: CLI via console e SSH;

2.5.43. A solução de gerenciamento deve possuir, no mínimo, três níveis de usuários: Administrador; Usuário com permissões reduzidas; e usuário Somente Leitura;

2.5.44. A solução de WAF e a solução de balanceamento de carga entre aplicações web do TRF6 deverão permitir que mais de um usuário possa estar conectado simultaneamente a interface de administração com a permissão de leitura/escrita;

2.5.45. A solução não deverá ter nenhum limite de licença para a quantidade de usuários ou dispositivos que poderão ser configurados. O único limite que será permitido é de capacidade do processamento dos appliances dentro dos throughputs e quantidade de requisições solicitados;

2.5.46. Deverá permitir autenticação dos usuários em bases remotas como, no mínimo, Microsoft Active Directory, RADIUS e OpenLDAP;

2.5.47. A interface gráfica de gerenciamento deverá permitir a atualização do sistema operacional e/ou a instalação de patches ou Hotfixes sem o uso da linha de comando;

2.5.48. Utilizar SCP ou HTTPS como mecanismo de transferência de arquivos de configuração e Sistema Operacional;

2.5.49. A interface Gráfica deverá permitir a reinicialização do equipamento;

2.5.50. A Solução de gerenciamento deve possuir uma única console que permita a organização, gerenciamento, configuração e aplicação das políticas de segurança, regras de balanceamento, aceleração, cache em todos os equipamentos que compõem a solução de WAF com balanceamento;

2.5.51. A Gerência deve ter capacidade de obter e analisar eventos em tempo real;

2.5.52. A Solução de gerenciamento deve fornecer as seguintes funcionalidades no seu ambiente gráfico:

2.5.52.1. Adição, alteração ou remoção de aplicações a serem protegidas pelo firewall de proteção a aplicações Web;

2.5.52.2. Adição, alteração ou remoção de regras de balanceamento, aceleração e cache;

2.5.52.3. Obter e analisar eventos em tempo real e gerar relatórios durante a avaliação do tráfego;

2.5.52.4. Permitir utilizar as informações obtidas para refinar as políticas de segurança a qual gerou o evento;

2.5.52.5. Permitir a criação de listas de acesso baseadas em endereços IP. Deve ser possível definir os endereços IP de origem das sessões.

2.5.53. Deve manter internamente múltiplos arquivos de configurações do sistema;

2.5.54. Deve permitir a exportação e importação de regras e políticas para um novo dispositivo de forma simples;

2.5.55. Deve permitir o armazenamento de sua configuração em memória não volátil, no caso de uma queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação;

2.5.56. Deve suportar rollback de configuração e imagem;

2.5.57. Deve possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, traceroute, ping e log de eventos;

2.5.58. O sistema operacional do dispositivo deverá permitir a utilização da ferramenta tcpdump, ou similar de qualidade igual ou superior, para captura e monitoração de pacotes em quaisquer de suas interfaces de rede, permitindo que as capturas sejam armazenadas em formato libpcap;

2.5.59. A execução do tcpdump, ou ferramenta similar, não deve impactar no desempenho dos appliances. Permitir a definição de funcionalidades e dados requeridos por auditores;

2.5.60. O armazenamento dos demais dias poderá ser local ou remoto;

2.5.61. Possuir configuração de múltiplos syslog servers para os quais o equipamento irá enviar as mensagens de syslog;

2.5.62. Possuir agente de gerenciamento SNMP, MIB SNMP II, extensões MIB SNMP, MIB bridging (RFC 1493), que possua descrição completa da MIB implementada no equipamento, inclusive as extensões privadas, se existirem;

2.5.63. Suporte ao protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol).

2.6. Capacitação Técnica

2.6.1. O treinamento deverá ser completo para contemplar a instalação, customização, operação e administração da solução de WAF para 5 (cinco) funcionários da CONTRATANTE, na modalidade de Ensino a Distância (EAD), online e ao vivo;

2.6.2. O treinamento deverá ser ministrado para turma especifica para a CONTRATANTE;

2.6.3. Serão aceitos cursos oficiais do fabricante da solução;

2.6.4. Deverá possuir módulos teóricos e práticos;

2.6.5. Os instrutores devem ser certificados pelo fabricante da solução para o treinamento;

2.6.6. O conteúdo dos cursos deverá abranger, minimamente, os seguintes tópicos:

2.6.6.1. Configuração – acesso e navegação na solução; comando de configurações básicas e avançadas; estrutura/arquitetura do sistema operacional dos equipamentos; configuração via CLI, GUI, Client e web;

2.6.6.2. Operação e troubleshooting avançado – comandos de gerenciamento e monitoramento da saúde dos recursos dos equipamentos; aplicação de bloqueios manuais e automáticos e criação de filtros;

2.6.7. É obrigatório relacionar a ementa dos cursos, carga horária e conteúdo programático. A abordagem do treinamento deve ser eminentemente prática, utilizando exemplos e exercícios para ilustrar os conceitos e capacitar os participantes a empregar os recursos oferecidos;

2.6.8. Ao final do treinamento deve ser emitido certificado de conclusão para cada participante/aluno constando a carga horária e a ementa

2.7. Software e Licenciamento

2.7.1. Todas as licenças que compõem a solução deverão ser de propriedade da CONTRATANTE e permitir a plena continuidade de utilização e operação da solução mesmo após o término do contrato, de forma perpétua.

2.7.2. As assinaturas da solução de WAF devem ser atualizadas durante o período do contrato sem que seja necessário nenhum custo adicional por parte da CONTRATANTE na aquisição de novas licenças ou subscrições.

2.8. Instalação e Configuração

2.8.1. O serviço de instalação e configuração deverá ser executado por técnico certificado pelo fabricante;

2.8.2. O serviço de instalação compreende as atividades de planejamento, instalação física, instalação lógica e finalização da solução no ambiente da CONTRATADA;

2.8.3. O serviço de configuração consiste em ajustar todos os parâmetros necessários (físicos e lógicos) para o funcionamento da solução e a sua adequação para funcionamento no ambiente da CONTRATADA atendendo aos requisitos dessa especificação.

2.9. Operação Assistida

2.9.1. A operação assistida deverá ocorrer durante 45 (quarenta e cinco) dias corridos a partir da instalação e configuração da solução na CONTRATANTE;

2.9.2. O serviço de operação assistida é composto por um conjunto de atividades que permitem o treinamento e a capacitação da equipe da CONTRATANTE responsável pelas atividades de operação, manutenção preventiva e corretiva, transferindo todo o conhecimento e experiência necessária para a operação da solução;

2.9.3. Durante os 45 dias corridos, será prestado todo o suporte necessário para a operacionalidade da solução, minimizando o risco da implantação da solução e proporcionando as condições ideais para transferência da tecnologia envolvida em regime de treinamento enquanto trabalha, até que a CONTRATANTE possa assumir as atividades com sua própria equipe;

2.9.4. Durante a operação assistida também será necessário realizar, pela CONTRADADA, possíveis customizações e ajustes finais que forem identificados durante o período de instalação, configuração e operação assistida;

2.9.5. Por padrão, a prestação da operação assistida ocorrerá presencialmente nas dependências da CONTRATANTE ou remotamente a ser definido pela CONTRATANTE.

2.10. Suporte, Manutenção e Atualização de Versão

2.10.1. O suporte técnico compreende o diagnóstico e identificação de problemas, apoio técnico na utilização, correção de erros, defeitos (bugs) ou mau funcionamento sobre qualquer funcionalidade, recurso, componente ou módulo disponível de forma nativa na solução de WAF e balanceamento, ou decorrente de qualquer adaptação (customização) e ajuste (tuning) efetuada pela CONTRATANTE;

2.10.2. O atendimento a um chamado de suporte deverá ocorrer por qualquer uma das seguintes formas: contato telefônico, envio de mensagem eletrônica (e-mail), acesso ao sítio (website) da CONTRATADA ou do fabricante da solução de WAF, com controle de acesso por senha;

2.10.3. O atendimento telefônico sempre que aplicável e viável, por meio de ligação local em Belo Horizonte/MG ou ligação interurbana gratuita (0800) e deverá ter um único número de contato para todos os produtos de software que compõem a solução de WAF;

2.10.4. A CONTRATANTE poderá efetuar um número ilimitado de chamados técnicos para a CONTRATADA, por qualquer uma das formas disponíveis, durante vigência do contrato vinculado a este edital;

2.10.5. Na abertura ou registro de um chamado técnico, por qualquer uma das formas disponíveis, a CONTRATADA deverá informar: data e hora de abertura do chamado, descrição do chamado, nível de severidade do chamado e identificação completa do solicitante;

2.10.6. A CONTRATADA deverá retornar, via e-mail, a confirmação da abertura do chamado técnico, doravante denominado confirmação do chamado, contemplando as seguintes informações na sua abertura: código de identificação do chamado, identificação do responsável da CONTRATADA pela abertura do chamado;

2.10.7. O atendimento ao chamado técnico pela CONTRATADA deverá ocorrer pelo menos por uma das seguintes formas: chamada telefônica, envio de mensagem eletrônica (e-mail), recursos disponíveis no sítio (site) do fabricante da solução de WAF ou da CONTRATADA, presencial ou suporte por acesso remoto;

2.10.8. Caso acionado o suporte direto do fabricante, este deverá ter atendimento em português. Caso contrário, a CONTRATADA deverá ser responsável por intermediar os contatos entre o fabricante e a CONTRATANTE;

2.10.9. Um chamado técnico somente será considerado contingenciado ou concluído com o aceite da CONTRATANTE, na forma de um visto na ordem de serviço correspondente ou aceite por e-mail ou ainda, diretamente no sistema oferecido pela CONTRATADA, caso esta forma seja utilizada;

2.10.10. Após apresentar uma solução de contorno para o chamado técnico, a CONTRATADA deverá retornar, via e-mail, a confirmação da execução do serviço, contemplando as seguintes informações: código de identificação do chamado, data e hora de conclusão do atendimento, descrição dos serviços executados e/ou da solução apresentada;

2.10.11. Em caso de adoção de solução de contorno, sem prejuízo da solução definitiva cabível, a CONTRATADA deverá emitir laudos, na periodicidade exigida pela CONTRATANTE, informando sobre a evolução dos trabalhos para solucionar o problema de forma definitiva;

2.10.12. Após apresentar uma solução definitiva para o CHAMADO TÉCNICO, a CONTRATADA deverá retornar, via e-mail, a confirmação da execução do serviço, contemplando as seguintes informações: código de identificação do chamado, data e hora de conclusão do atendimento, descrição dos serviços executados e/ou da solução apresentada;

2.10.13. Deverá ser garantido à CONTRATANTE o pleno acesso ao sítio (site) dos fabricantes dos produtos que compõem a solução de WAF, com direito a consultas a quaisquer bases de conhecimentos e fóruns de discussão disponíveis para seus usuários;

2.10.14. Caberá exclusivamente à CONTRATANTE a decisão de implantar ou não quaisquer atualizações de software fornecidos pela CONTRATADA;

2.10.15. A CONTRATADA deverá disponibilizar mecanismos para a atualização de software pelo download direto através da própria aplicação, pelo envio das mídias ou através de download no seu sítio (site) ou do fabricante do software em questão;

2.10.16. O serviço de manutenção consiste na correção de qualquer problema ou falha apresentados em componentes físicos ou lógicos da solução;

2.10.17. A atualização de software é uma alteração da versão anterior com o objetivo de implementar melhorias. Essas melhorias podem ser de usabilidade, correção de falhas, desempenho, adição de novas funcionalidades, etc.;

2.10.18. O prazo de atualização de todo software fornecido deve ser igual ao período de garantia do produto. Durante a vigência do contrato, a CONTRATANTE terá direito a todas atualizações de versão e release dos softwares.

2.11. Garantia

2.11.1. O(s) equipamento(s) que compõe(m) a solução devem estar em sua versão mais atual até a data de assinatura do contrato e a data de final de suporte (end-of-support) deve ocorrer após o término da vigência contratual da solução;

2.11.2. O serviço de Garantia contempla garantir o correto e pleno funcionamento de todos os itens adquiridos necessários para o funcionamento da solução, incluindo atualizações regulares de segurança e patches para proteger contra novas vulnerabilidades e ameaças;

2.11.3. Prazo de garantia deverá ser de 60 meses.

3. LOTE 3. SERVIÇO DE SEGURANÇA DE BORDA (SERVICE SECURITY EDGE - SSE)

3.1. Características Gerais da Solução

3.1.1. O SSE deve possuir os seguintes componentes:

3.1.1.1. Acesso à Rede Zero Trust (ZTNA): O ZTNA;

3.1.1.2. Agente de segurança de acesso à nuvem (CASB);

3.1.1.3. Gateway seguro da web (SWG).

3.1.2. A solução deve ser fornecida com licenças para 4500 usuários, com validade de 60 meses, incluindo todas as funcionalidades e atualizações necessárias durante o período de assinatura a fim de assegurar o acesso à internet e a aplicativos para usuários remotos;

3.1.3. A solução deve ser construída com uma arquitetura nativa em nuvem e entregue como um serviço (SaaS), garantindo alta disponibilidade, escalabilidade e manutenção contínua sem interrupções significativas para os usuários finais;

3.1.4. O serviço deve possuir infraestrutura de filtragem web (proxy) em datacenter localizado no território brasileiro, sendo permitida a replicação desta infraestrutura em outros países;

3.1.5. A inspeção do conteúdo de conexões originadas no Brasil deve ser feita em datacenter dentro do território brasileiro;

3.1.6. Visando a disponibilidade e redundância do serviço, a CONTRATADA deverá oferecer em sua plataforma, pelo menos, 2 (dois) datacenters em território brasileiro;

3.1.7. Todas as funcionalidades deverão ser ofertadas na nuvem como serviço. A nuvem deverá ser distribuída globalmente, incluindo o Brasil, e deverá ser licenciada para, pelo menos, 4.500 (quatro mil e quinhentos) usuários;

3.1.8. A solução deverá prover no mínimo 2 (dois) endereços exclusivos para TRF6 (/31) para acesso à Internet por datacenter no Brasil, de forma a garantir a saída por apenas com IPs designados para os Datacenters posicionados no Brasil;

3.1.9. O datacenter localizado no Brasil deverá ter conectividade redundante ao PTT (Ponto de Troca de Tráfego) no Brasil, peering estabelecido com provedores de serviços, empresas de telecomunicações, CDNs (Content Delivery Network) e provedores de nuvem pública tais como (AWS, Microsoft e Google). Desta forma, será possível garantir melhor experiência e baixa latência aos usuários;

3.1.10. O datacenter do fabricante localizado no Brasil deve possuir, no mínimo, 2 (dois) links com velocidade superior a 50Gbps no principal ponto de troca do Brasil (IX.BR);

3.1.11. O fabricante deve possuir infraestrutura em território brasileiro, não sendo aceitas soluções como:

3.1.11.1. Virtualização de appliances em nuvens públicas;

3.1.11.2. Pontos de presença instalados em nuvens de terceiros como AWS, Azure, GCP e outros.

3.1.12. O datacenter do fabricante localizado em território nacional não deve armazenar as informações das transações em disco local. Os dados referentes as transações devem ser compactados, tokenizados e exportados para uma estrutura apartada de armazenamento de logs, que deverá ser prevista nesta contratação, através de conexões TLS seguras.

3.1.13. Não serão aceitos sistemas baseados em hardware ou software projetados para uso genérico, ou de código aberto (*open source*);

3.1.13.1. Os elementos ofertados não podem ser customizados.

3.1.14. A solução deve oferecer uma interface de administração centralizada e intuitiva, permitindo o gerenciamento eficiente das políticas de segurança, configurações de usuários e análise de relatórios de acesso e autenticação;

3.1.15. O serviço deve garantir a disponibilidade mensal mínima de 99,7%, assegurando-se a máxima confiabilidade e tempo de atividade do sistema;

3.1.16. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

3.1.17. Deve consolidar múltiplos serviços de segurança para controle de acesso à Internet, como DNS, Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Remote Browser Isolation (RBI);

3.1.18. O agente instalado deve ser capaz de identificar quando estiver conectado à internet de maneira remota, ou por dentro da infraestrutura do escritório remoto. Para com isso ser ativado/desativado de acordo com a política.

3.1.19. A solução não deve depender de cliente instalado na máquina do usuário. Para o acesso agentlesss, deve suportar, no mínimo, os seguintes tipos de aplicações:

3.1.19.1. Web;

3.1.19.2. SSH;

3.1.19.3. RDP;

3.1.19.4. VNC, Team Viewer ou AnyDesk, entre outros.

3.1.20. Toda a comunicação entre o usuário e a plataforma deve ser realizada através de conexões TLS;

3.1.21. Deve ser compatível os seguintes provedores de identidade: Okta, Azure AD ou Active Directory / LDAP; SAML 2.0 Identity Providers; Auth0, Google Workspace e Workday;

3.1.22 Deve possuir base de inteligência do próprio fabricante, que inclua recursos de Inteligência Artificial (IA), estatística e modelos de aprendizado de máquina para fornecer informações sobre ameaças de cibersegurança ameaças e melhorar as taxas de resposta a incidentes;

3.1.23. A solução deve permitir a implementação de respostas automáticas ou guiadas a incidentes, minimizando o impacto de ameaças detectadas;

3.1.24. A solução deve oferecer integração rápida com plataformas de comunicação como Slack e Microsoft Teams, facilitando a notificação imediata de incidentes;

3.1.25. Deve ser compatível com plataformas de Information Event Management (SIEM) e Security Orchestration, Automation and Response (SOAR), permitindo uma análise de segurança aprofundada e resposta automatizada a incidentes;

3.1.26. O portal deve ser uma extensão da solução de Single Sign-On, permitindo que os usuários entrem uma única vez e obtenham acesso a todas as aplicações autorizadas sem a necessidade de autenticações adicionais devendo também permitir a configuração de login único (SSO) para acesso através da integração com um provedor de identidade (IdP) compatível com SAML 2.0 Identity Providers, Okta, AzureAD, Active Directory / LDAP, Google Workspace.

3.1.27. A validação de postura para máquinas Windows deve contemplar pelo menos a validação de:

3.1.27.1. Antivírus instalado;

3.1.27.2. Certificados;

3.1.27.3. Processos em execução;

3.1.27.4. Versão de SO.

3.1.28. A validação de postura também deverá se aplicar ao acesso *agentless* (sem agentes), não apenas ao acesso com cliente instalado no dispositivo do usuário.

3.1.29. A validação de postura para o acesso agentless deve comtemplar no mínimo as seguintes validações:

3.1.29.1. Data e hora de acesso;

3.1.29.2. IP;

3.1.29.3. Localização (País de acesso);

3.1.29.4. SO.

3.1.30. O client deve estar disponível para o seguintes Sistemas Operacionais:

3.1.30.1. Windows (exe e msi);

3.1.30.2. Linux (Ubuntu, Red Hat e Fedora);

3.1.30.3. Android / Chromebook;

3.1.30.4. iOS.

3.2. Módulo de Gerenciamento

3.2.1. Deve prover console em nuvem, para todas as funções próprias da solução sendo aceita composição de solução do mesmo fabricante;

3.2.2. Deve permitir extrair logs a partir de soluções externas, como SIEM;

3.2.3. Deve possuir autenticação via protocolo SAML, permitindo integrar com provedores de serviços de identidade (IdP) para acesso administrativo à console;

3.2.4. Deve suportar APIs para gerenciamento com, no mínimo, as seguintes funcionalidades:

3.2.4.1. Autenticação;

3.2.4.2. Provisionamento;

3.2.4.3. Gestão de Políticas;

3.2.4.4. Relatórios.

3.2.5. Deve possuir ao menos três níveis de usuário: Administrador completo, Administrador de segurança e Apenas leitura;

3.2.6. Prover painel com informações sumarizadas de navegação de usuários contendo quantidade de sessões ativas e consumo de banda através de uma linha do tempo;

3.2.6.1. A gerência centralizada e monitoração deve possibilitar a visualização dos logs de Firewall, navegação web e prevenção de ameaças;

3.2.6.2. Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento.

3.3. Segurança de Acesso - Política de Acesso

3.3.1. Deve usar o conceito de política de acesso unificada, sem políticas separadas para DNS, Secure Web Gateway (SWG);

3.3.2. Deve permitir ações de Bloqueio, Permissão, Alerta e Isolamento (Remote Browser Isolation);

3.3.3. Deve permitir a criação de páginas personalizadas de bloqueio e alerta, com opção de contato com administrador;

3.3.4. Deve permitir especificar origens a serem usadas na política de acesso internet, com base em:

3.3.4.1. Usuários/Grupos através de integração com Microsoft Active Directory ou provedores de identidade via SAML, tais como Azure AD e Okta;

3.3.5. Deve permitir especificar destinos a serem usados na política de acesso internet, com base em:

3.3.5.1. Listas personalizadas de domínios, URLs, IPs/Redes, incluindo a capacidade de fazer o upload destas;

3.3.5.2. IP/Redes, Portas e Protocolos (Any, UDP, TCP, ICMP);

3.3.5.3. Categorias de conteúdo web ou listas personalizadas de categorias.

3.3.5.4. Aplicações ou listas personalizadas de aplicações.

3.3.6. Deve aplicar uma regra de acesso internet padrão e customizável, caso o fluxo não seja mapeado em outra regra;

3.3.7. Deve possuir contador de visitas (Hit count), indicando quantas vezes uma regra foi acionada.

3.4. Segurança de Acesso Internet - Camada DNS

3.4.1. Deve possuir infraestrutura global de resolução recursiva de DNS para proteção de acesso à internet;

3.4.2. Não deve ser uma solução para configuração, manutenção, implementação e serviço de DNS autoritativo;

3.4.3. Não deve ser uma solução para substituição de infraestrutura DNS interno, serviço DHCP;

3.4.4. Deve oferecer proteção para dispositivos de rede internos e externos;

3.4.5. Deve possuir suporte a IPv6 para DNS;

3.4.6. Deve permitir os seguintes métodos de envio de tráfego DNS:

3.4.6.1. Integração nativa com o sistema de DNS atual do ambiente de produção, substituindo as referências de servidores recursivos externos em uso.

3.4.7. Deve permitir visibilidade e controle de acesso a domínios, por meio de classificação por categorias;

3.4.8. Deve permitir a definição de listas personalizadas de acesso a domínios, para permissão (allow lists) e para bloqueio (block lists) incluindo a capacidade de fazer o upload destas;

3.4.9. Deve ser capaz de identificar e bloquear requisições de acesso a domínios que estejam classificados, no mínimo, nas categorias de segurança abaixo:

3.4.9.1. Malware;

3.4.9.2. Command and Control (C&C);

3.4.9.3. Phishing;

3.4.9.4. DNS dinâmico;

3.4.9.5. Cryptomining;

3.4.9.6. Domínios novos ou vistos pela primeira vez, por, no mínimo, 24h;

3.4.9.7. DNS Tunneling;

3.4.9.8. Domínios suspeitos ou potencialmente maliciosos.

3.5. Gateway Seguro da Web - Secure Web Gateway (SWG)

3.5.1. A solução deverá identificar automaticamente tráfegos Web em portas não padrão (80 e 443) e realizar a inspeção Web completa, incluindo inspeção SSL e todas as funcionalidades de controle de acesso e segurança, mesmo em uma arquitetura de proxy transparente.

3.5.2. Deve permitir visibilidade e controle de acesso a URLs, por meio de classificação por categorias;

3.5.3. Deve permitir visibilidade e controle de acesso a URLs não categorizadas pelo fabricante;

3.5.4. Deve permitir a definição de listas personalizadas de acesso a domínios, URLs e IPs, para permitir (allow lists) e para bloqueio (block lists) incluindo a capacidade de fazer o upload destas;

3.5.5. Deve suportar descriptografia TLS/HTTPS completa ou seletiva, com suporte a Certificate Authority (CA) do próprio cliente;

3.5.6. Deve permitir excluir categorias de conteúdo, aplicações e domínios do processo de descriptografia (descriptografia seletiva);

3.5.7. Deve suportar descriptografia e inspeção de TLS 1.2 e 1.3;

3.5.8. Deve possuir recurso de antivírus/anti-malware para escaneamento de arquivos em trânsito;

3.5.9. Deve possuir mecanismo automático de envio de arquivos para malware sandboxing;

3.5.10. Deve permitir os seguintes métodos de envio de tráfego Secure Web Gateway(SWG):

3.5.10.1. Arquivo PAC (Proxy Auto-Configuration);

3.5.10.2. Túnel Ipsec;

3.5.10.3. Encaminhamento de tráfego com cliente para máquinas windows, macOS, linux e android;

3.5.11. Deve possuir controle granular (Upload e/ou Download) de aplicações web, suportando ao menos:

3.5.11.1. Box;

3.5.11.2. X (Twitter);

3.5.11.3. Dropbox;

3.5.11.4. Pinterest;

3.5.11.5. Messenger;

3.5.11.6. Gmail;

3.5.11.7. Facebook;

3.5.11.8. Linkedin;

3.5.11.9. Slack;

3.5.11.10. Instagram;

3.5.11.11. Google Drive;

3.5.11.12. SlideShare;

3.5.11.13. YouTube;

3.5.11.14. Vimeo;

3.5.11.15. WhatsApp;

3.5.11.16. SmartSheet;

3.5.11.17. Pastebin;

3.5.11.18. WeTransfer.

3.6. Agente de segurança de acesso à nuvem (CASB):

3.6.1. Deve ser capaz de monitorar a utilização de serviço em nuvem (Cloud Services) para identificar riscos e desenvolver atividades de conformidade (Shadow IT);

3.6.2. Deve possuir relatórios sobre a categoria do fornecedor, nome do aplicativo e volume de atividade para cada aplicativo descoberto;

3.6.3. Deve incluir detalhes do aplicativo e informações de risco, como pontuação de reputação na Web, viabilidade financeira e certificações de conformidade relevantes;

3.6.4. Deve possuir capacidade de bloquear/permitir aplicativos específicos;

3.6.5. Deve possuir recurso de detecção, quarentena e/ou remoção de malware em aplicativos baseados em nuvem, via API, no mínimo para os seguintes aplicativos:

3.6.5.1. Dropbox;

3.6.5.2. Box;

3.6.5.3. Webex Teams;

3.6.5.4. Microsoft 365;

3.6.5.5. Google Drive.

3.6.6. Deve possuir opção de restrições de locatário (Tenant Controls) para permitir acesso apenas a instâncias de aplicativos SaaS indicados pelo administrador, suportando, no mínimo, os seguintes aplicativos:

3.6.6.1. Microsoft 365;

3.6.6.2. Google G Suite;

3.6.6.3. Slack;

3.6.6.4. Dropbox.

3.7. Remote Browser Isolation (RBI)

3.7.1. Deve possuir funcionalidade de isolamento remoto de browser para proteção contra potenciais ameaças e malware, através do direcionamento do tráfego HTTPS a um serviço de browser protegido em nuvem;

3.7.2. A funcionalidade de RBI deve ser acionada como opção de ação a ser tomada nas regras para destinos e identidades selecionados;

3.7.3. A funcionalidade de RBI deve poder ser acionada para destinos considerados arriscados, como sites não categorizados e categorias de ameaça de segurança;

3.7.4. A funcionalidade de RBI deve poder ser acionada para qualquer destino, categoria ou aplicação suportada pelo serviço de proxy;

3.7.5. O RBI deve suportar os seguintes navegadores:

3.7.5.1. Apple Safari;

3.7.5.2. Google Chrome;

3.7.5.3. Microsoft Edge;

3.7.5.4. Mozilla Firefox.

3.7.6. O RBI deve suportar autenticação de terceiros (ex. Dropbox usando Google para autenticação).

3.8. Data Loss Prevention (DLP)

3.8.1. Deve possuir camada múltipla de DLP para dados em trânsito (em tempo real) e em repouso (via API);

3.8.2. Deve permitir a classificação de dados sensíveis através de uso individual ou combinado de dicionários pré- definidos e personalizados;

3.8.3. Deve permitir a classificação de dados sensíveis através de dicionários personalizados com opção de termos, frases e padrões via expressões regulares;

3.8.4. Deve permitir configurar diferentes níveis de severidade por regra;

3.8.5. Deve permitir inspecionar os arquivos por nome, conteúdo ou ambos;

3.8.6. O DLP deve suportar, no mínimo, os seguintes tipos de arquivos:

3.8.7.1. Word .doc e .docx;

3.8.7.2. PDF;

3.8.7.3. RTF;

3.8.7.4. Excel .xls e .xlsx;

3.8.7.5. PowerPoint .ppt e .pptx;

3.8.7.6. OpenDocument presentation .odp;

3.8.7.7. OpenDocument sheet .ods;

3.8.7.8. OpenDocument word .oth;

3.8.7.9. E-mail;

3.8.7.10. CSV;

3.8.7.11. HTML/XML;

3.8.7.12. Texto .txt;

3.8.7.13. TSV;

3.8.7.14. URL.

3.8.8. O DLP para dados em trânsito deve ter opções de alerta e bloqueio para dados expostos em arquivos, formulários web e aplicações web;

3.8.9. O DLP para dados em trânsito de suportar os seguintes tipos de formulários (forms):

3.8.9.1. JSON;

3.8.9.2. XML;

3.8.9.3. URL encoded;

3.8.9.4. Multipart form.

3.8.10. O DLP para dados em trânsito deve ter, no mínimo, os seguintes serviços para inspeção:

3.8.10.1. Box Cloud Storage;

3.8.10.2. ChatGPT;

3.8.10.3. Concur Invoice;

3.8.10.4. Confluence;

3.8.10.5. Dropbox;

3.8.10.6. Facebook Messenger;

3.8.10.7. Gmail;

3.8.10.8. Jira;

3.8.10.9. Linkedin SlideShare;

3.8.10.10. Monday;

3.8.10.11. PasteBin;

3.8.10.12. SalesForce;

3.8.10.13. ServiceNow;

3.8.10.14. ShareFile;

3.8.10.15. Slack;

3.8.10.16. SmartSheet;

3.8.10.17. WeTransfer;

3.8.10.18. WorkDay;

3.8.10.19. Yahoo Mail.

3.8.11. Deve permitir especificar as identidades a serem usadas na política de DLP de dados em trânsito, com base em:

3.8.12. O DLP para dados em repouso deve permitir varredura de arquivos compartilhados, pelo menos, nas seguintes aplicações:

3.8.12.1. Microsoft 365 OneDrive e Sharepoint;

3.8.12.2. Microsoft Teams;

3.8.12.3. Google Drive e Meet.

3.8.13. O DLP para dados em repouso deve dar opções de ação de monitorar e revogar acesso;

3.8.14. O DLP para dados em repouso deve permitir especificar o escopo de varredura para todos os usuários ou usuários específicos.

3.9. Acesso à Rede Zero Trust (ZTNA)

3.9.1. Deve usar o conceito de política de acesso unificada, sem políticas separadas para ZTNA;

3.9.2. Deve permitir ações de Bloqueio e Permissão;

3.9.3. Deve permitir especificar origens a serem usadas na política de acesso privado, com base em:

3.9.3.1. Usuários/Grupos através de integração com Microsoft Active Directory ou provedores de identidade via SAML, tais como Azure AD e Okta.

3.9.4. Deve permitir especificar destinos a serem usados na política de acesso a recursos privados, com base em:

3.9.4.1. Aplicações internas previamente configuradas, de forma individual ou global.

3.9.5. Deve permitir especificar requisitos de dispositivo de origem a serem usadas na política de acesso privado, com base em:

3.9.5.1. Postura do dispositivo gerenciado ou não conforme política;

3.9.5.2. Requisitos de autenticação recorrente de usuário.

3.9.6. Deve aplicar uma regra padrão que negue acesso privado, caso o fluxo não seja mapeado em outra regra;

3.9.7. Deve possuir contador de visitas (Hit count), indicando quantas vezes uma regra foi acionada;

3.9.8. Deve permitir habilitar e desabilitar regras individualmente;

3.9.9. Suportar descriptografia para inspeção de tráfego privado.

3.10. Conector de recursos privados do ZTNA

3.10.1. A solução deve possibilitar conexões rápidas e seguras a redes e aplicações privadas, por meio de máquinas virtuais (VMs) implantadas à frente das aplicações privadas, que forneçam conectividade de dentro para fora. Deve ser possível instalar nos ambientes:

3.10.1.1. On-premises através de uma imagem VMWare ESXi (ova);

3.10.1.2. Nuvem AWS;

3.10.1.3. Nuvem Azure;

3.10.1.4. Nuvem Google.

3.10.2. Deve ter a capacidade de suportar conexão DTLS e TLS;

3.10.2.1. Deve regredir para a conexão TLS, caso DTLS seja bloqueado;

3.10.3. Deve ter a capacidade de calcular o número de instâncias baseado no throughput de tráfego estimado;

3.11. ZTNA com Agente

3.11.1. Deve ter a capacidade de acessar recursos privados utilizando qualquer protocolo;

3.11.2. Deve permitir a aplicação de políticas de postura do usuário, incluindo os seguintes requisitos:

3.11.2.1. Verificação do sistema operacional e a versão;

3.11.2.2. Verificação de um agente de segurança no dispositivo;

3.11.2.3. Verificação de senha no dispositivo;

3.11.2.4. Verificação do navegador utilizado e sua versão.

3.11.3. Deve rotear o tráfego baseado no IP/FQDN da aplicação destino;

3.12. ZTNA sem Agente (via browser)

3.12.1. Deve ser possível acessar aplicações privadas sem agente instalado;

3.12.2. Deve ter a capacidade de gerar um FQDN resolvível publicamente;

3.12.3. Deve ter a capacidade de autenticação via SAML;

3.12.4. Deve ter a capacidade de prover conexão a recursos privados para dispositivos não gerenciados BYOD;

3.12.5. Deve ter a capacidade de selecionar os navegadores permitidos;

3.12.6. Deve ter a capacidade de selecionar os sistemas operacionais permitidos.

3.13. Painéis e Relatórios

3.13.1. Deve possuir painel de visão geral do ambiente, incluindo informações de, pelo menos:

3.13.1.1. Gráfico com volume de tráfego (total, enviado e recebido) agregado e por método de conexão no período selecionado;

3.13.1.2. Atividade de segurança (solicitações e bloqueios) e principais categorias de segurança visitadas por dispositivos e usuários no período selecionado;

3.13.1.3. Conexões de rede privada ZTNA ao longo do tempo, listando usuários com maior número de solicitações no período selecionado;

3.13.1.4. Número de vezes que os aplicativos internos foram acessados, número de usuários que solicitaram acesso e o número de solicitações permitidas ou bloqueadas durante o período selecionado;

3.13.1.5. Número de vezes que cada método de acesso (ZTNA com cliente, ZTNA sem cliente) foi utilizado e recursos internos mais utilizados no período selecionado.

3.13.2. Deve prover, no mínimo, os seguintes relatórios:

3.13.2.1. Todas as atividades de acesso durante um determinado período de tempo ajustável, relacionadas a segurança ou não, com filtros, no mínimo, por tipo de evento, camada responsável pela detecção, ação tomada, identidade usada no acesso, destino, categoria de segurança e categoria de conteúdo;

3.13.2.2. Todas as atividades de acesso relacionadas a segurança durante um determinado período de tempo ajustável, com filtros, no mínimo, por tipo de evento, ação tomada, identidade usada no acesso, destino e categoria de segurança;

3.13.2.3. Visão sobre aplicativos Web descobertos (Shadow IT), indicando fornecedor, categoria, nome, volume de atividade, risco, certificações de conformidade relevantes e identidades usadas nos acessos;

3.13.2.4. Destinos mais acessados num período determinado de tempo ajustável, relacionados a segurança ou não, com filtros, no mínimo, por camada responsável pela detecção, ação tomada, identidade usada no acesso,

categoria de segurança e categoria de conteúdo;

3.13.2.5. Categorias mais acessadas num período determinado de tempo ajustável, relacionadas a segurança ou não, com filtros, no mínimo, por camada responsável pela detecção, ação tomada e identidade usada no acesso;

3.13.2.6. Atividades executadas na console da solução, indicando usuário responsável, data e hora, IP de origem, área do produto relacionada e ação executada, com possibilidades de filtro, no mínimo, por usuário, período de

tempo e IP;

3.13.2.7. Visão geral dos arquivos maliciosos identificados nas plataformas SaaS integradas ao ambiente, indicando total de arquivos escaneados, total de malwares detectados, total de usuários com malware, data e hora da detecção, com filtros, no mínimo, por plataforma, nível de exposição, status e nome do arquivo. Deve possibilitar ações de isolar em quarentena e restaurar arquivos;

3.13.2.8. Violações de dados (DLP) detectadas em tempo real e via API, indicando data e hora do evento, regra acionada, identidade envolvida, nome do arquivo e URL de destino, com filtros, no mínimo, por tipo (real time ou API), ação tomada, severidade, aplicação, nível de exposição, identidade e hash de arquivos. Deve indicar, nos detalhes do evento, trecho do conteúdo de texto exposto que acionou a regra, com as devidas máscaras para a parte mais sensível do texto.

3.13.3. Todos os dados disponíveis para a consulta e criação de relatórios deverão residir no plano de gestão por, no mínimo, 30 dias;

3.13.4. Deve permitir exportar relatórios para arquivos CSV, JSON, HTML ou outro formato capaz de manipulação;

3.13.5. Deve permitir agendamento e envio automático de relatórios.

3.14. Monitoramento de Experiência Digital:

3.14.1. Deve incluir, de forma unificada na console administrativa, área para monitoramento de experiência digital com medição de desempenho e a disponibilidade em tempo real de dispositivos, aplicativos e serviços, auxiliando na resolução de problemas e melhoria de produtividade;

3.14.2. Deve possuir, ao menos, os seguintes recursos de monitoramento:

3.14.2.1. Disponibilidade e desempenho de dispositivos em tempo real, indicando consumo de CPU, memória, disco, sinal WIFI, latência, jitter e perda de pacotes;

3.14.2.2. Análise da rota de comunicação de dados entre os dispositivos de usuários até o serviço contratado;

3.14.2.3. Mapa da infraestrutura de rede, fornecendo informações sobre a distribuição geográfica, conectividade e situação dos dispositivos;

3.14.2.4. Disponibilidade e desempenho do principal aplicativo de colaboração cadastrado, com opção para, pelo menos, Webex, Zoom e Microsoft Teams;

3.14.2.5. Desempenho e a disponibilidade de acesso aos aplicativos SaaS mais comuns, tais como AWS, Microsoft 365 e Google Suite.

3.15. Capacitação Técnica

3.15.1. O treinamento deverá ser completo para contemplar a instalação, customização, operação e administração da solução de SSE para 5 (cinco) funcionários da CONTRATANTE, na modalidade de Ensino a Distância (EAD), online e ao vivo;

3.15.2. O treinamento deverá ser ministrado para turma especifica para a CONTRATANTE;

3.15.3. Serão aceitos cursos oficiais do fabricante da solução.

3.16. Instalação e Configuração

3.16.1. O serviço de instalação e configuração deverá ser executado por técnico certificado pelo fabricante;

3.16.2. O serviço de instalação compreende as atividades de planejamento, instalação física, instalação lógica e finalização da solução no ambiente da CONTRATADA;

3.16.3. O serviço de configuração consiste em ajustar todos os parâmetros necessários (físicos e lógicos) para o funcionamento da solução e a sua adequação para funcionamento no ambiente da CONTRATADA atendendo aos requisitos dessa especificação.

3.17. Operação Assistida

3.17.1. A operação assistida deverá ocorrer durante 45 (quarenta e cinco) dias corridos a partir da instalação e configuração da solução na CONTRATANTE;

3.17.2. O serviço de operação assistida é composto por um conjunto de atividades que permitem o treinamento e a capacitação da equipe da CONTRATANTE responsável pelas atividades de operação, manutenção preventiva e corretiva, transferindo todo o conhecimento e experiência necessária para a operação da solução;

3.17.3. Durante os 45 dias corridos, será prestado todo o suporte necessário para a operacionalidade da solução, minimizando o risco da implantação da solução e proporcionando as condições ideais para transferência da tecnologia envolvida em regime de treinamento enquanto trabalha, até que a CONTRATANTE possa assumir as atividades com sua própria equipe;

3.17.4. Durante a operação assistida também será necessário realizar, pela CONTRADADA, possíveis customizações e ajustes finais que forem identificados durante o período de instalação, configuração e operação assistida;

3.17.5. Por padrão, a prestação da operação assistida ocorrerá presencialmente nas dependências da CONTRATANTE ou remotamente a ser definido pela CONTRATANTE.

3.18. Suporte, Manutenção e Atualização de Versão

3.18.1. O suporte técnico compreende o diagnóstico e identificação de problemas, apoio técnico na utilização, correção de erros, defeitos (bugs) ou mau funcionamento sobre qualquer funcionalidade, recurso, componente ou módulo disponível de forma nativa efetuada pela CONTRATANTE;

3.18.2. O atendimento a um chamado de suporte deverá ocorrer por qualquer uma das seguintes formas: contato telefônico, envio de mensagem eletrônica (e-mail), acesso ao sítio (website) da CONTRATADA ou do fabricante da solução, com controle de acesso por senha;

3.18.3. A CONTRATANTE poderá efetuar um número ilimitado de chamados técnicos para a CONTRATADA, por qualquer uma das formas disponíveis, durante vigência do contrato vinculado a este Termo de Referência;

3.18.4. Caso acionado o suporte direto do fabricante, este deverá ter atendimento em português. Caso contrário, a CONTRATADA deverá ser responsável por intermediar os contatos entre o fabricante e a CONTRATANTE.

b) Plano de Sustentação

1. O plano de sustentação tem como objeto permitir o funcionamento adequado e contínuo de ambiente crítico de Infraestrutura de TIC, durante e após a execução do objeto, e ainda após o encerramento do contrato.

2. Recursos necessários à continuidade do negócio

2.1. Recursos Materiais

Recurso	Qtde.	Disponibilidade	Ação para obtenção do Recurso	Responsável
Espaço	1	Entrega da Solução	Obter espaço para guarda dos novos equipamentos até que a troca seja efetuada. Local para armazenar os equipamentos antigos até que seja feita o desfazimento. Espaço disponível no galpão.	SEMAP

2.2. Recursos Humanos

Função	Formação	Período	Atribuições
Gestor e Fiscais do Contrato	Designados por Portaria	Assinatura do Contrato	Fazer reunião inicial com a CONTRATADA para alinhamento da execução contratual, apresentação das equipes responsáveis pela execução e fiscalização, análise dos pontos críticos da execução e levantamento de fatores que possam impactar a execução do objeto.
Fiscais Requisitantes e Técnicos		Da assinatura até o recebimento definitivo da solução	Repassar as informações técnicas para elaboração do plano de implantação. Receber o plano de implantação, analisar e propor as correções técnicas necessárias se for o caso. Aprovar o plano de implantação, com os ajustes propostos. Acompanhar a instalação da solução. Apoiar as comissões de recebimento quanto a quesitos técnicos.
Comissão de Recebimento Provisório		Recebimento	Controlar o prazo para entrega da solução. Receber e conferir os objetos entregues se em conformidade com a proposta aprovada. Emitir documentos de não conformidade, em caso de objetos divergentes. Emitir termo de recebimento provisório, identificando os bens entregues, cumprimento dos prazos contratados e atestando a conformidade com a proposta.
Comissão de Recebimento Definitivo		Instalação, Configuração e Migração	Acompanhar e controlar os prazos contratados previstos para cada etapa de execução, até a emissão do Termo de Recebimento Definitivo. Fiscalizar o processo de instalação, configuração e migração. Emitir documentos de não conformidade, em caso de divergência observada. Acompanhar os testes de compatibilidade da solução com as especificações técnicas do Edital.

			Conferir, validar e aprovar os produtos e serviços executados. Atestar a instalação e configuração mediante emissão de Termo de Recebimento Definitivo.
Fiscais Requisitantes e Técnicos		Recebimento definitivo até fim de vigência do contrato	Acompanhar e fiscalizar a execução dos serviços e anotar em registro próprio todas as ocorrências relacionadas com a execução, sob os aspectos quantitativos e qualitativos, comunicando as ocorrências de quaisquer fatos que exijam medidas corretivas por parte da contratada. Determinar as datas e os horários para realização das manutenções, prevendo o mínimo de impacto nas atividades dos usuários. Abrir chamados para solicitação de suporte. Analisar e verificar se os níveis de qualidade contratados foram alcançados e aplicar as glosas estipuladas para cada caso.
Gestor do Contrato		Vigência Contratual	Autorizar a aplicação das glosas/descontos propostas pelos fiscais. Encaminhar a documentação comprobatória de penalizações ou multas administrativas para os setores responsáveis e solicitar providências.

2.3. Continuidade da Solução de TIC

2.3.1. A continuidade de prestação dos serviços de rede é um dos objetivos principais da contratação proposta.

Evento	Tipo de Ação	Ação	Responsáveis
Inexecução ou má prestação nos serviços de manutenção pela CONTRATADA	Preventiva	Acompanhamento do cumprimento das obrigações contratuais.	Comissões de Recebimento e Gestor do Contrato
	Preparação	Reunir equipe de planejamento para contratação, preparando nova documentação para licitação de empresa que possa dar continuidade na manutenção ou no fornecimento de nova solução substituta.	Fiscal Técnico, Gestor do Contrato
	Contingência	Avaliar possibilidade de contratação de fornecedor remanescente da licitação. Iniciar ações para contratação emergencial. Preparar documentação para nova licitação	Fiscal Demandante, Fiscal Técnico e Gestor do Contrato
Falência da empresa ou rescisão por descumprimento de obrigações contratuais (inexecução total do contrato)	Preventiva	Acompanhamento das sanções/multas administrativas no decorrer do contrato. Verificar junto à CONTRATADA sua qualificação econômico-financeira, que minimize a ocorrência do risco de falência da empresa.	Gestão do contrato
	Preparação	Desenvolvimento de novo edital para contratação de outra empresa.	Equipe de Planejamento
	Contingência	Contratação emergencial de empresa especializada para as manutenções corretivas.	Gestor do Contrato e SECTI
Encerramento normal do Contrato	Preventiva	Por se tratar de ambiente crítico que necessita de manutenção continuada, preventiva e reativa, preparar nova contratação para dar continuidade aos serviços de manutenção.	Fiscal Demandante, Gestor do Contrato
	Preparação	Desenvolvimento de edital para nova contratação.	Equipe de Planejamento da Contratação e Gestor do Contrato
	Contingência	Contratação emergencial de empresa especializada para as manutenções corretivas.	Gestor do Contrato, SECTI

2.4. Transição Contratual

2.4.1. Avaliação de Continuidade Contratual

Ação	Formação	Início	Final
Avaliar mensalmente os serviços prestados no período e os resultados obtidos, efetuando os descontos, desconsiderações e multas necessárias quando for o caso, para resultados não conformes.	Fiscais e Gestor do Contrato	Assinatura do Contrato	Encerramento da Vigência
Acompanhar os serviços e exigir a transferência de conhecimento entre as equipes de colaboradores técnicos e a CONTRATADA.	Fiscal Técnico	Assinatura do Contrato	Encerramento da Vigência

2.4.2. Ações para Encerramento Contratual

Ação	Formação	Início	Final
Analisar a existência de atualização de versionamentos, fixes e evoluções dos softwares e hardwares da solução e solicitar as correções finais.	Fiscal Técnico	30 dias antes do fim da vigência do contrato	Encerramento da Vigência
Executar a transferência de conhecimento entre as equipes de colaboradores técnicos do atual fornecedor de serviços para a nova CONTRATADA, de forma a minimizar a possibilidade de interrupção ou degradação	Fiscais e Gestor do Contrato	30 dias antes do fim da	Encerramento da Vigência

na operação e prestação desses serviços no âmbito do TRF6.		vigência do contrato	
Os custos de desmobilização para encerramento do contrato correrão por conta do TRF6.	Gestor do Contrato	Dia seguinte ao encerramento do contrato	Devolução da garantia contratual
Elaborar documentos e avisos para comunicar à SECTI e à SUINF que a Contratada não possuirá mais acesso para manutenção no ambiente do SECTI.	Gestor do Contrato	30 dias antes do fim da vigência do contrato	Dia seguinte ao encerramento do contrato
Efetuar o descadastramento das contas de serviço da contratada, impedindo acesso às instalações e equipamentos da SECTI.	Fiscal Técnico	Dia seguinte ao encerramento do contrato	Dia seguinte ao encerramento do contrato
Garantir que todas as manutenções previstas no plano até a data de encerramento do contrato sejam atualizadas.	Fiscais Requisitante e Técnico	30 dias antes do fim da vigência do contrato	Encerramento da Vigência
Solicitar à administração a liberação da garantia contratual.	Gestor do Contrato	Encerramento do Contrato	Dois meses após encerramento do contrato

2.5. Estratégia de Independência

2.5.1. Transferência de conhecimento

Atividade	Forma de Transferência
Documentação do projeto da solução	Documentação atualizada do projeto da solução, compartilhada entre todos os integrantes da equipe.
Encontro de alinhamento Técnico	Realização de encontros técnicos, quando necessário, com a equipe técnica do CONTRATANTE responsável pela gestão da solução, para a transferência de conhecimento acerca das atividades.
Procedimento de instalação e configuração	Todas as instalações, configurações e manutenções deverão ser registradas e documentadas em procedimentos internos, para que possam ser reproduzidos e divulgados com a equipe técnica.
Descrição das entregas de serviços	Todas as construções de produtos através da prestação de serviços deverão ser entregues acompanhadas de descrição completa, para documentação técnica e regras de negócio.
Relatório de atividades	Em todo atendimento para manutenções no ambiente, deverá ser entregue um relatório com a descrição da atividade realizada.
Direitos de Propriedade Intelectual	Todos os produtos advindos da execução contratual, não se limitando aos documentos descritivos da solução, diagramas de conexão, “as-builts”, rotinas de migração e rotinas computacionais desenvolvidas, são de propriedade exclusiva do TRF6. Tais produtos deverão ter tratamento confidencial por parte da CONTRATADA, que não poderá divulgá-los a terceiros sem o expresso consentimento do Tribunal.

VIII - Justificativas para o parcelamento ou não da contratação

( ) Não se aplica em razão da licitação ser dispensável ou inexigível.

( ) Não é possível o parcelamento, pois trata-se de apenas 1 (um) item. (ADJUDICAÇÃO: MENOR PREÇO POR ITEM).

(X) É possível a contratação da solução de forma divisível observado o §2 do art. 40 da Lei n. 14.133/2021 (ADJUDICAÇÃO: MENOR PREÇO POR LOTES).

( ) Todos ou alguns itens da solução devem ser agrupados para o fornecimento por um único fornecedor, observado o §3º do art. 40 da Lei nº 14.133/2021

(ADJUDICAÇÃO: MENOR PREÇO GLOBAL).

Justificativa:

Justifica-se a divisão do objeto em lotes em razão da interdependência entre os equipamentos e serviços que compõem o objeto da contratação, considerando-se o grau de interação do conjunto de serviços técnicos, assim como a sua natureza específica e o seu caráter contínuo, aliada à alta criticidade e à complexidade da infraestrutura apoiada.

As melhores práticas na implantação de uma nova solução de segurança se baseiam na integração das soluções e serviços, que são indissociáveis e apresentam inter-relação entre si, de forma que assegurem o alinhamento e a coerência em termos de qualidade técnica, resultando assim, no perfeito atendimento dos princípios da celeridade, economicidade e eficiência.

O fracionamento da solução em itens avulsos poderia expor a diversos riscos a qualidade e a disponibilidade do ambiente tecnológico da JF6, já que não seria possível delimitar as responsabilidades, tarefas e ações caso haja mais de um fornecedor dentro do processo de execução dos serviços.

A definição de um lote único, por sua vez, impede a disputa entre fabricantes e prestadores com *know-how* para os lotes da presente contratação, uma vez que somente um deles se mostrou capaz de atender a todo o objeto.

Seguem abaixo algumas considerações técnicas adicionais para o parcelamento do objeto em lotes:

- A pesquisa de mercado identificou somente um fabricante capaz de atender a todo o objeto da contratação, logo a divisão por lotes possibilita a maior concorrência entre os interessados e, consequentemente, a maior economicidade;

- Quando analisado sob os aspectos técnicos, percebe-se o inter-relacionamento e a interdependência entre os serviços e equipamentos a serem contratados, daí a impossibilidade de estabelecimento dos limites, por serem extremamente tênues, de início e término das repercussões entre um e outro. Destacam-se as metas de alcance de maturidade, alta disponibilidade e a gestão de riscos de um mesmo ambiente de infraestrutura, para qual cada atividade contribuirá em aspectos distintos;
- Para a adequada execução dos serviços ora contratados é fundamental que esteja assegurada a unidade conceitual de todas as etapas técnicas, que a cada lote compõe um todo uno e indivisível, entrelaçado com coerência tecnológica e direcionado para o resultado esperado que é a disponibilidade do ambiente de infraestrutura de TI, incluídos todos os aspectos necessários ao pleno atendimento das necessidades dos usuários destes serviços;
- A indivisibilidade do lote é imprescindível, pois tecnicamente e gerencialmente é inviável que os serviços sejam fornecidos por diferentes contratadas, uma vez que traz ônus direto de maior custo gerencial para controle, além do maior custo gerencial para gestão contratual, constituindo todos estes benefícios em vantajosidade técnica e economicidade;
- No tocante à economicidade, particionar em itens poderia impactar diretamente os custos globais da contratação, uma vez que a execução dos serviços por um único prestador por lote tende a permitir ganhos de escala e possibilita a diluição do custo do *overhead* administrativo por um maior número de profissionais alocados para atendimento dos serviços. A gestão e a fiscalização de um número maior de contratos para a execução dos serviços de infraestrutura aumentariam também os custos indiretos com recursos humanos da CONTRATANTE a serem alocados para tal atividade;
- Contratar prestadores distintos para o fornecimento de produto e a execução dos serviços de um lote poderia trazer conflitos de responsabilidades entre as contratadas, prejudicando sobremaneira a execução contratual e a fiscalização por parte da CONTRATANTE;
- Por tudo exposto e considerando a interdependência entre o itens e lotes determinados, entende-se incabível a reserva de cotas para ME/EPP prevista no art. 48, III da Lei Complementar n. 123, de 2006, sob pena de incorrer em prejuízo ao conjunto do objeto a ser contratado.

Por tudo exposto e em virtude da especificidade do objeto, pode-se afirmar que é tecnicamente inadequado o seu desmembramento por itens, sob pena de não se atender ao objetivo buscado, assim como o estabelecimento de lote único, em razão da falta de concorrência. Sob o ponto de vista econômico, não há elementos nos autos que permitam concluir que a adoção do parcelamento do objeto por itens ou a definição de lote único seriam, no caso concreto, mais vantajosos para o TRF6.

IX - Demonstrativo dos resultados pretendidos em termos de economicidade e de melhor aproveitamento dos recursos humanos, materiais e financeiros disponíveis

Busca-se com a presente contratação:

a) Atualizar o parque tecnológico do TRF6;

b) Obter serviços de alta disponibilidade;

c) Aumentar a velocidade de operação entre os equipamentos;

d) Otimizar o desempenho da rede de dados;

e) Garantir a estabilidade operacional das comunicações do TRF6 e suas subseções judiciárias;

f) Aumentar a proteção de rede do TRF6, possibilitando a inspeção de tráfego com maior granularidade que a atualmente realizada;

g) Melhorar o desempenho e eficácia no controle de acesso ao perímetro de rede através de equipamentos com níveis de processamento e capacidade mais adequados;

h) Aumentar a disponibilidade das aplicações, evitando o comprometimento da capacidade do firewall em eventuais situações de ataque;

i) Possuir viabilidade para realizar futuras expansões da capacidade e granularidade da rede do Tribunal;

j) Possibilitar a ampliação da segmentação da rede com o objetivo de reduzir os riscos de segurança;

k) Aumento da resiliência em caso de ataques;

l) Diminuir o tempo de análise e resolução de problemas.

X - Providências a serem adotadas pela Administração previamente à celebração do contrato, inclusive quanto à capacitação de servidores ou de empregados para fiscalização e gestão contratual

Não se aplica.

XI - Contratações correlatas e/ou interdependentes

Não se aplica.

XII - Descrição de possíveis impactos ambientais e respectivas medidas mitigadoras, incluídos requisitos de baixo consumo de energia e de outros recursos, bem como logística reversa para desfazimento e reciclagem de bens e refugos, quando aplicável

12.1. Critérios:

12.1.1. Tenho conhecimento de que: A fabricante e/ou distribuidora, e/ou importadora, e/ou comerciante e/ou consumidora deste objeto deve possuir Cadastro Técnico Federal de Atividades Potencialmente Poluidoras e/ou Utilizadoras de Recursos Ambientais (CTF/APP)?

a) (X) Não. ( ) Sim. Identifique a(s) categoria(s) da Ficha Técnica de Enquadramento (FTE): _____

b) ( ) a fabricante, e/ou distribuidora, e/ou importadora, e/ou comerciante, e/ou consumidora deste objeto não se enquadra nas FTEs do CTF/APP.

12.1.2. Os produtos/objetos são constituídos de material (marque quantos itens forem necessários):

( ) renovável ( ) reciclado ( ) atóxico ( ) biodegradável (X) não se aplica

12.1.3. Os objetos são considerados produtos perigosos, segundo a Gestão de Resíduos Sólidos do TRF6/SJMG:

(X) Não. ( ) Sim. Quais? _____

12.1.4. Os objetos da aquisição devem estar em conformidade com os seguintes regulamentos técnico/legal: (marque quantos itens forem necessários):

( ) Etiqueta Nacional de Conservação de Energia

( ) Certificado de Conformidade de Potência Sonora de Produtos Eletrodomésticos

( ) Certificado de Vistoria de Veículo

( ) Ficha de Informações de Segurança de Produtos Químicos

( ) Documento de Origem Florestal

( ) Autorização para o Exercício da Atividade de Revenda de GLP

( ) Outro(s). Especificar: _____

12.1.5. Há outros critérios de sustentabilidade, além dos relacionados acima:

(X) Não. ( ) Sim. Descreva: _____

12.2. Deverão ser consideradas as diretivas do Plano de Logística Sustentável do TRF6, normativos internos e a legislação vigente.

12.2.1. A aquisição ou contratação demandará ou resultará em (marque quantos itens forem necessários)

(X) geração de resíduo.

( ) consumo de papel.

( ) consumo de outros materiais de expediente (caneta, grampos, clips, pastas etc).

( ) consumo de café ou açúcar.

( ) consumo de água mineral envasada.

( ) gastos com correspondências.

( ) instalação de computador ou impressora.

( ) aparelho de telefone fixo ou móvel.

(X) consumo de energia elétrica.

( ) consumo de água.

( ) serviços de engenharia (instalações elétricas, hidráulicas, ponto de rede, ponto de telefone, divisórias).

( ) obras civis (reforma ou construção de edificação).

( ) serviço de limpeza - aumento da área a ser limpa no TRF6.

( ) serviço de vigilância - aumento no número de postos.

( ) quantidade de veículos na frota do TRF6.

( ) gasto com contratos de veículos (manutenção, peças, insumos, seguro, lavagem, terceirização, exceto motorista).

( ) consumo de combustível.

( ) ação de qualidade de vida.

( ) ação de capacitação socioambiental.

( ) não demandará ou resultará em nenhum dos itens acima.

XIII - Posicionamento conclusivo sobre a adequação da contratação para o atendimento da necessidade a que se destina

Com base nas informações levantadas ao longo deste estudo técnico, declaramos que a solução apresentada é viável de prosseguir e ser concretizada, pois é a que melhor atende os requisitos técnicos e funcionais pretendidos pela área demandante.

Certificamos que somos responsáveis pela elaboração do presente documento que compila os Estudos Técnicos Preliminares e que este traz os conteúdos previstos na Lei nº 14.133/2021.

Na redação foram observadas as diretrizes estabelecidas no Guia de Contratações de TIC, instituídas pela Resolução CNJ nº 468/2022 (art. 16 da IN STJ/GDG n. 4/2023).

13.1. A Equipe de Planejamento da Contratação foi instituída pela Portaria TRF6-SECOF 10/2024 (0779055).

Responsáveis pela elaboração:

Integrante Requisitante	Integrante Técnico	Integrante Administrativo
Nome: Heli Lopes Rios Diretor da Subsecretaria de Infraestrutura - SUINF / SECTI Matrícula: TR 38	Nome: Arianne Caldeira do Carmo Diretora do Núcleo de Defesa Cibernética e Tratamento de Incidentes de Segurança da Informação - NUDCI Matrícula: TR 587	Nome: Fernanda Marília Gonçalves Caetano Assessor I - SULIC Matrícula: TR 578
O presente planejamento está em conformidade com os requisitos técnicos necessários ao cumprimento do objeto e atende adequadamente às demandas de negócio formuladas. Os benefícios pretendidos são adequados, os riscos envolvidos são administráveis, os custos previstos são compatíveis e caracterizam a economicidade.		

Responsável pela revisão, supervisão e controle de qualidade:

Autoridade Máxima da Área de TI
Nome: Daniel Santos Rodrigues Diretor da Secretaria de Tecnologia da Informação - SECTI/TRF6 Matrícula: TR 44
O presente planejamento está em conformidade com os requisitos técnicos necessários ao cumprimento do objeto e atende adequadamente às demandas de negócio formuladas. Os benefícios pretendidos são adequados, os riscos envolvidos são administráveis, os custos previstos são compatíveis e caracterizam a economicidade, **pelo que aprovo o artefato e encaminho para prosseguimento da contratação**.

Documento assinado eletronicamente por **Heli Lopes Rios**, **Diretor(a) de Subsecretaria**, em 06/11/2024, às 13:30, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Arianne Caldeira do Carmo**, **Diretor(a) de Núcleo**, em 06/11/2024, às 13:33, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Fernanda Marília Gonçalves Caetano**, **Assessor(a) I**, em 06/11/2024, às 14:42, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Daniel Santos Rodrigues**, **Diretor(a) de Secretaria**, em 06/11/2024, às 15:18, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.trf6.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0990939** e o código CRC **AC2700C7**.

PODER JUDICIÁRIO
TRIBUNAL REGIONAL FEDERAL DA 6ª REGIÃO
Seção de Licitações

ATA DE REGISTRO DE PREÇOS MINUTA - TRF6-SELIT

ATA DE REGISTRO DE PREÇOS MINUTA - TRF6

Nº ____/2025

PREGÃO ELETRÔNICO 90017/2024 - TRF6

O Tribunal Regional Federal da 6ª Região, CNPJ 47.784.477/0001-79 , com sede na Av. Álvares Cabral, 1.805, Bairro Santo Agostinho, Belo Horizonte/MG, neste ato representado pelo seu Diretor-Geral, no uso de suas atribuições, conforme delegação contida no art. 1º, XXI, da Portaria Presi 103/2022, considerando o julgamento do **Pregão Eletrônico 90017/2024 - TRF6**, para registro de preços, publicado no Diário Oficial da União de _____, **processo administrativo 0006130-19.2024.4.06.8000**, RESOLVE registrar os preços da(s) empresa(s) indicada(s) e qualificada(s) nesta ATA, de acordo com a classificação por ela(s) alcançada(s) e na(s) quantidade(s) cotada(s), atendendo as condições previstas no Edital deste Pregão, sujeitando-se as partes às normas constantes da Lei 14.133/2021 e do Decreto 11.462/2023 e em conformidade com as disposições a seguir.

1. DO OBJETO

1.1. A presente Ata tem por objeto o registro de preços para aquisição de solução de segurança de TIC com a finalidade de atender às necessidades de funcionamento dos sistemas do Tribunal Regional Federal da 6ª Região, conforme condições, quantidades e exigências estabelecidas no Edital e seus anexos.

2. DOS PREÇOS, ESPECIFICAÇÕES E QUANTITATIVOS

2.1. O preço registrado, as especificações do objeto, as quantidades de cada item, fornecedor e as demais condições ofertadas na proposta são as que seguem:

Beneficiária:
CNPJ:
Endereço:
Telefone:
Representante:
Endereço eletrônico:

GRUPOS	ITENS	SERVIÇOS	UNIDADES REFERENCIAIS	QUANTIDADES
01	01	Appliances de Next Generation Firewall	Unidade	2
	02	Licenciamentos para operações de Next Generation Firewall por 60 meses	Conjunto	1
	03	Instalação e Configuração	Conjunto	1
	04	Suporte Técnico por 60 (sessenta) meses	Mensal	60
	05	Treinamento	Turma	1
02	06	Web Application Firewall - Appliance Virtual	Unidade	1
	07	Instalação e Configuração	Conjunto	1
	08	Suporte Técnico por 60 (sessenta) meses	Mensal	60
	09	Treinamento	Turma	1
03	10	Serviço de Segurança de Borda (Security Service Edge - SSE)	Usuários	12.650
	11	Instalação e Configuração	Conjunto	8
	12	Suporte Técnico por 60 (sessenta) meses	Mensal	480
	13	Treinamento	Turma	8

2.2. A listagem do cadastro de reserva referente ao presente registro de preços consta como anexo a esta Ata.

3. ÓRGÃO GERENCIADOR E PARTICIPANTE(S)

3.1 Para o **ÓRGÃO GERENCIADOR**, os preços registrados, as especificações do objeto e as quantidades ofertadas na proposta são:

GRUPOS	ITENS	CATMAT / CATSER	SERVIÇOS	UNIDADES REFERENCIAIS	QUANTIDADES	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)	VALOR TOTAL DO GRUPO (R$)
01	01	484747	Appliances de Next Generation Firewall	Unidade	2			
	02	27472	Licenciamentos para operações de Next Generation Firewall por 60 meses	Conjunto	1			
	03	26972	Instalação e Configuração	Conjunto	1			
	04	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60			
	05	3840	Treinamento	Turma	1			
02	06	27472	Web Application Firewall - Appliance Virtual	Unidade	1			
	07	26972	Instalação e Configuração	Conjunto	1			
	08	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60			
	09	3840	Treinamento	Turma	1			
03	10	27742	Serviço de Segurança de Borda (Security Service Edge - SSE)	Usuários	4.500			
	11	26972	Instalação e Configuração	Conjunto	1			
	12	27740	Suporte Técnico por 60 (sessenta) meses	Mensal	60			
	13	3840	Treinamento	Turma	1			

3.2 São **ÓRGÃOS PARTICIPANTES** do registro de preços:

a) Tribunal Regional Federal da 4ª Região;

b) Seção Judiciária do Paraná;

c) Seção Judiciária do Rio Grande do Sul;

d) Seção Judiciária de Santa Catarina;

e) Seção Judiciária do Ceará;

f) Seção Judiciária do Rio Grande do Norte;

g) Seção Judiciária de Sergipe.

3.3. Para os **ÓRGÃOS PARTICIPANTES**, os preços registrados, as especificações do objeto e as quantidades

ofertadas na proposta são:

TRIBUNAL REGIONAL FEDERAL DA 4ª REGIÃO

GRUPO	ITENS	SERVIÇOS	UNIDADES REFERENCIAIS	QUANTIDADES	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)
3	10	Serviço de Segurança de Borda (Security Service Edge - SSE)	Usuários	1.250		
	11	Instalação e Configuração	Conjunto	1		
	12	Suporte Técnico por 60 (sessenta) meses	Mensal	60		
	13	Treinamento	Turma	1		

SEÇÃO JUDICIÁRIA DO PARANÁ

GRUPO	ITENS	SERVIÇOS	UNIDADES REFERENCIAIS	QUANTIDADES	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)
3	10	Serviço de Segurança de Borda (Security Service Edge - SSE)	Usuários	2.500		
	11	Instalação e Configuração	Conjunto	1		
	12	Suporte Técnico por 60 (sessenta) meses	Mensal	60		
	13	Treinamento	Turma	1		

SEÇÃO JUDICIÁRIA DO RIO GRANDE DO SUL

GRUPO	ITENS	SERVIÇOS	UNIDADES REFERENCIAIS	QUANTIDADES	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)
3	10	Serviço de Segurança de Borda (Security Service Edge - SSE)	Usuários	150		
	11	Instalação e Configuração	Conjunto	1		
	12	Suporte Técnico por 60 (sessenta) meses	Mensal	60		
	13	Treinamento	Turma	1		

SEÇÃO JUDICIÁRIA DE SANTA CATARINA

GRUPO	ITENS	SERVIÇOS	UNIDADES REFERENCIAIS	QUANTIDADES	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)
3	10	Serviço de Segurança de Borda (Security Service Edge - SSE)	Usuários	1.450		
	11	Instalação e Configuração	Conjunto	1		
	12	Suporte Técnico por 60 (sessenta) meses	Mensal	60		
	13	Treinamento	Turma	1		

SEÇÃO JUDICIÁRIA DO CEARÁ

GRUPO	ITENS	SERVIÇOS	UNIDADES REFERENCIAIS	QUANTIDADES	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)

3	10	Serviço de Segurança de Borda (Security Service Edge - SSE)	Usuários	1.400		
	11	Instalação e Configuração	Conjunto	1		
	12	Suporte Técnico por 60 (sessenta) meses	Mensal	60		
	13	Treinamento	Turma	1		

SEÇÃO JUDICIÁRIA DO RIO GRANDE DO NORTE

GRUPO	ITENS	SERVIÇOS	UNIDADES REFERENCIAIS	QUANTIDADES	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)
3	10	Serviço de Segurança de Borda (Security Service Edge - SSE)	Usuários	1.000		
	11	Instalação e Configuração	Conjunto	1		
	12	Suporte Técnico por 60 (sessenta) meses	Mensal	60		
	13	Treinamento	Turma	1		

SEÇÃO JUDICIÁRIA DE SERGIPE

GRUPO	ITENS	SERVIÇOS	UNIDADES REFERENCIAIS	QUANTIDADES	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)
3	10	Serviço de Segurança de Borda (Security Service Edge - SSE)	Usuários	400		
	11	Instalação e Configuração	Conjunto	1		
	12	Suporte Técnico por 60 (sessenta) meses	Mensal	60		
	13	Treinamento	Turma	1		

4. DA ADESÃO À ATA DE REGISTRO DE PREÇOS

4.1. Durante a vigência da ata, os órgãos e as entidades da Administração Pública federal, estadual, distrital e municipal **poderão** aderir à ata de registro de preços, observados os seguintes requisitos:

4.1.1. apresentação de justificativa da vantagem da adesão, inclusive em situações de provável desabastecimento ou descontinuidade de serviço público;

4.1.2. demonstração de que os valores registrados estão compatíveis com os valores praticados pelo mercado na forma do art. 23 da Lei nº 14.133, de 2021; e

4.1.3. consulta e aceitação prévias do órgão ou da entidade gerenciadora e do fornecedor.

4.2. A autorização do órgão ou entidade gerenciadora apenas será realizada após a aceitação da adesão pelo fornecedor.

4.2.1. O órgão ou entidade gerenciadora poderá rejeitar adesões caso elas possam acarretar prejuízo à execução de seus próprios contratos ou à sua capacidade de gerenciamento.

4.3. Após a autorização do órgão ou da entidade gerenciadora, o órgão ou entidade não participante deverá efetivar a aquisição ou a contratação solicitada em até noventa dias, observado o prazo de vigência da ata.

4.4. O prazo de que trata o subitem anterior, relativo à efetivação da contratação, poderá ser prorrogado excepcionalmente, mediante solicitação do órgão ou da entidade não participante aceita pelo órgão ou pela entidade gerenciadora, desde que respeitado o limite temporal de vigência da ata de registro de preços.

4.5. O órgão ou a entidade poderá aderir a item da ata de registro de preços da qual seja integrante, na qualidade de não participante, para aqueles itens para os quais não tenha quantitativo registrado, observados os requisitos do item 4.1.

Dos limites para as adesões

4.6. As aquisições ou contratações adicionais não poderão exceder, por órgão ou entidade, a cinquenta por cento dos quantitativos dos itens do instrumento convocatório registrados na ata de registro de preços para o gerenciador e para os participantes.

4.7. O quantitativo decorrente das adesões não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para o gerenciador e os participantes, independentemente do número de órgãos ou entidades não participantes que aderirem à ata de registro de preços.

4.8. A adesão à ata de registro de preços por órgãos e entidades da Administração Pública estadual, distrital e municipal poderá ser exigida para fins de transferências voluntárias, não ficando sujeita ao limite de que trata o item 4.7, desde que seja destinada à execução descentralizada de programa ou projeto federal e comprovada a compatibilidade dos preços registrados com os valores praticados no mercado na forma do art. 23 da Lei nº 14.133, de 2021.

Vedação a acréscimo de quantitativos

4.9. É vedado efetuar acréscimos nos quantitativos fixados na ata de registro de preços.

5. VALIDADE, FORMALIZAÇÃO DA ATA DE REGISTRO DE PREÇOS E CADASTRO DE RESERVA

5.1. **A validade da Ata de Registro de Preços será de 1 (um) ano**, contado a partir do primeiro dia útil subsequente à data de divulgação no PNCP, **podendo ser prorrogada por igual período**, com a renovação de seus quantitativos, mediante a anuência do fornecedor, **desde que comprovado o preço vantajoso**, conforme art. 84 da Lei 14.133/2021.

5.1.1. O contrato decorrente da ata de registro de preços terá sua vigência estabelecida no próprio instrumento contratual e observará, no momento da contratação e a cada exercício financeiro, a disponibilidade de créditos orçamentários, bem como a previsão no plano plurianual, quando ultrapassar 1 (um) exercício financeiro.

5.1.2. Na formalização do contrato ou do instrumento substituto, deverá haver a indicação da disponibilidade dos créditos orçamentários respectivos.

5.2. A contratação com os fornecedores registrados na ata será formalizada pelo órgão ou pela entidade interessada por intermédio de instrumento contratual, emissão de nota de empenho de despesa, autorização de compra ou outro instrumento hábil, conforme o art. 95 da Lei 14.133/2021.

5.2.1. O instrumento contratual de que trata o subitem 5.2. deverá ser assinado no prazo de validade da ata de registro de preços.

5.3. Os contratos decorrentes do sistema de registro de preços poderão ser alterados, observado o art. 124 da Lei 14.133/2021.

5.4. Após a homologação da licitação, **deverão ser observadas as seguintes condições para formalização da ata de registro de preços:**

5.4.1. **Será incluído na ata, na forma de anexo**, o registro dos licitantes ou dos fornecedores que:

5.4.1.1. Aceitarem cotar os bens ou os serviços com preços iguais aos do adjudicatário, observada a classificação da licitação; e

5.4.1.2. Mantiverem sua proposta original.

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

5.5. O registro a que se refere o subitem 5.4.1 tem por objetivo a **formação de cadastro de reserva** para o caso de impossibilidade de atendimento pelo signatário da ata.

5.6. **Para fins da ordem de classificação**, os licitantes ou fornecedores que aceitarem reduzir suas propostas para o preço do adjudicatário antecederão aqueles que mantiverem sua proposta original.

5.7. A habilitação dos licitantes que comporão o cadastro de reserva a que se refere o subitem 5.5 somente será efetuada quando houver necessidade de contratação dos licitantes remanescentes, nas seguintes hipóteses:

5.7.1. Quando o licitante vencedor não assinar a ata de registro de preços, no prazo e nas condições estabelecidos no Edital; e

5.7.2. Quando houver o cancelamento do registro do licitante ou do registro de preços nas hipóteses previstas no item 9.

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

5.9. Após a homologação da licitação, o licitante mais bem classificado será convocado para assinar a ata de registro de preços, no prazo e nas condições estabelecidos no Edital, sob pena de decair o direito, sem prejuízo das sanções

previstas na Lei 14.133/2021.

5.9.1. O prazo de convocação poderá ser prorrogado 1 (uma) vez, por igual período, mediante solicitação do licitante ou fornecedor convocado, desde que apresentada dentro do prazo, devidamente justificada, e que a justificativa seja aceita pela Administração.

5.10. A ata de registro de preços será assinada por meio de assinatura digital e disponibilizada no Sistema de Registro de Preço.

5.11. Quando o convocado não assinar a ata de registro de preços no prazo e nas condições estabelecidas no Edital ou no aviso de contratação, e observado o disposto no subitem 5.7, fica facultado à Administração convocar os licitantes remanescentes do cadastro de reserva, na ordem de classificação, para fazê-lo em igual prazo e nas condições propostas pelo primeiro classificado.

5.12. Na hipótese de nenhum dos licitantes que trata o subitem 5.4.1.1, aceitar a contratação nos termos do subitem anterior, a Administração, observados o valor estimado e sua eventual atualização nos termos do Edital, poderá:

5.12.1. Convocar para negociação os demais licitantes ou fornecedores remanescentes cujos preços foram registrados sem redução, observada a ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário; ou

5.12.2. Adjudicar e firmar o contrato nas condições ofertadas pelos licitantes ou fornecedores remanescentes, atendida a ordem classificatória, quando frustrada a negociação de melhor condição.

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

6. ALTERAÇÃO OU ATUALIZAÇÃO DOS PREÇOS REGISTRADOS

6.1. **Os preços registrados poderão ser alterados ou atualizados** em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos bens, das obras ou dos serviços registrados, **nas seguintes situações:**

6.1.1. Em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução da ata tal como pactuada, nos termos da alínea “d” do inciso II do caput do art. 124 da Lei 14.133/2021;

6.1.2. Em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou a superveniência de disposições legais, com comprovada repercussão sobre os preços registrados;

6.1.3. Na hipótese de previsão no Edital de cláusula de reajustamento ou repactuação sobre os preços registrados, nos termos da Lei 14.133/2021.

6.1.3.1. No caso do reajustamento, deverá ser respeitada a contagem da anualidade e o índice previstos para a contratação;

6.1.3.2. No caso da repactuação, poderá ser a pedido do interessado, conforme critérios definidos para a contratação.

7. NEGOCIAÇÃO DE PREÇOS REGISTRADOS

7.1. **Na hipótese de o preço registrado tornar-se superior ao preço praticado no mercado por motivo superveniente**, o órgão gerenciador convocará o fornecedor para negociar a redução do preço registrado.

7.1.1. Caso não aceite reduzir seu preço aos valores praticados pelo mercado, o fornecedor será liberado do compromisso assumido quanto ao item registrado, sem aplicação de penalidades administrativas.

7.1.2. Na hipótese prevista no subitem anterior, o gerenciador convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam reduzir seus preços aos valores de mercado e não convocará os licitantes ou fornecedores que tiveram seu registro cancelado.

7.1.3. Se não obtiver êxito nas negociações, o órgão gerenciador procederá ao cancelamento da ata de registro de preços, adotando as medidas cabíveis para obtenção de contratação mais vantajosa.

7.1.4. Na hipótese de redução do preço registrado, o gerenciador comunicará aos órgãos e às entidades que tiverem firmado contratos decorrentes da ata de registro de preços para que avaliem a conveniência e a oportunidade de diligenciarem negociação com vistas à alteração contratual, observado o disposto no art. 124 da Lei 14.133/2021.

7.2. **Na hipótese de o preço de mercado tornar-se superior ao preço registrado e o fornecedor não poder cumprir as obrigações estabelecidas na ata**, será facultado ao fornecedor requerer ao gerenciador a alteração do preço registrado, mediante comprovação de fato superveniente que supostamente o impossibilite de cumprir o compromisso.

7.2.1. Neste caso, o fornecedor encaminhará, juntamente com o pedido de alteração, a documentação

comprobatória ou a planilha de custos que demonstre a inviabilidade do preço registrado em relação às condições inicialmente pactuadas.

7.2.2. Não hipótese de não comprovação da existência de fato superveniente que inviabilize o preço registrado, o pedido será indeferido pelo órgão gerenciador e o fornecedor deverá cumprir as obrigações estabelecidas na ata, sob pena de cancelamento do seu registro, nos termos do subitem 8.1, sem prejuízo das sanções previstas na Lei 14.133/2021, e na legislação aplicável.

7.2.3. Na hipótese de cancelamento do registro do fornecedor, nos termos do subitem anterior, o gerenciador convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam manter seus preços registrados, observado o disposto no subitem 5.7.

7.2.4. Se não obtiver êxito nas negociações, o órgão gerenciador procederá ao cancelamento da ata de registro de preços, nos termos do subitem 8.4, e adotará as medidas cabíveis para a obtenção da contratação mais vantajosa.

7.2.5. Na hipótese de comprovação da majoração do preço de mercado que inviabilize o preço registrado, conforme previsto nos subitens 7.2 e 7.2.1, o órgão gerenciador atualizará o preço registrado, de acordo com a realidade dos valores praticados pelo mercado.

7.2.6. O órgão gerenciador comunicará aos órgãos e às entidades que tiverem firmado contratos decorrentes da ata de registro de preços sobre a efetiva alteração do preço registrado, para que avaliem a necessidade de alteração contratual, observado o disposto no art. 124 da Lei 14.133/2021.

8. CANCELAMENTO DO REGISTRO DO LICITANTE VENCEDOR E DOS PREÇOS REGISTRADOS

8.1. **O registro do fornecedor será cancelado pelo órgão gerenciador, quando o fornecedor:**

8.1.1. Descumprir as condições da ata de registro de preços, sem motivo justificado;

8.1.2. Não retirar a nota de empenho, ou instrumento equivalente, no prazo estabelecido pela Administração sem justificativa razoável;

8.1.3. Não aceitar manter seu preço registrado, na hipótese prevista no artigo 27, § 2º, do Decreto 11.462/2023; ou

8.1.4. Sofrer sanção prevista nos incisos III ou IV do caput do art. 156 da Lei 14.133/2021.

8.1.4.1. Na hipótese de aplicação de sanção prevista nos incisos III ou IV do caput do art. 156 da Lei 14.133/2021, caso a penalidade aplicada ao fornecedor não ultrapasse o prazo de vigência da ata de registro de preços, poderá o órgão gerenciador, mediante decisão fundamentada, decidir pela manutenção do registro de preços, vedadas contratações derivadas da ata enquanto perdurarem os efeitos da sanção.

8.2. O cancelamento de registros nas hipóteses previstas no subitem 9.1 será formalizado por despacho do órgão gerenciador, garantidos os princípios do contraditório e da ampla defesa.

8.3. **Na hipótese de cancelamento do registro do fornecedor**, o órgão gerenciador poderá convocar os licitantes que compõem o cadastro de reserva, observada a ordem de classificação.

8.4. O cancelamento dos preços registrados poderá ser realizado pelo órgão gerenciador, em determinada ata de registro de preços, total ou parcialmente, nas seguintes hipóteses, desde que devidamente comprovadas e justificadas:

8.4.1. Por razão de interesse público;

8.4.2. A pedido do fornecedor, decorrente de caso fortuito ou força maior; ou

8.4.3. Se não houver êxito nas negociações, nas hipóteses em que o preço de mercado tornar-se superior ou inferior ao preço registrado, nos termos do artigos 26, § 3º e 27, § 4º, ambos do Decreto 11.462/2023.

9. REMANEJAMENTO DAS QUANTIDADES REGISTRADAS NA ATA DE REGISTRO DE PREÇOS

9.1. As quantidades previstas para os itens com preços registrados nas atas de registro de preços poderão ser remanejadas pelo órgão ou entidade gerenciadora entre os órgãos ou as entidades não participantes do registro de preços.

9.2. O órgão ou entidade gerenciadora que tiver estimado as quantidades que pretende contratar será considerado participante para efeito do remanejamento.

9.3. Na hipótese de remanejamento de órgão ou entidade participante para órgão ou entidade não participante, serão observados os limites previstos no art. 32 do Decreto nº 11.462, de 2023.

9.4. Competirá ao órgão ou à entidade gerenciadora autorizar o remanejamento solicitado, com a redução do quantitativo inicialmente informado pelo órgão ou pela entidade participante, desde que haja prévia anuência do órgão ou da entidade que sofrer redução dos quantitativos informados.

9.5. Caso o remanejamento seja feito entre órgãos ou entidades dos Estados, do Distrito Federal ou de Municípios distintos, caberá ao fornecedor beneficiário da ata de registro de preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento decorrente do remanejamento dos itens.

9.6. Na hipótese da compra centralizada, não havendo indicação pelo órgão ou pela entidade gerenciadora, dos quantitativos dos participantes da compra centralizada, nos termos do item 8.3, a distribuição das quantidades para a execução descentralizada será por meio do remanejamento.

10. DAS PENALIDADES

10.1. **O descumprimento da Ata de Registro de Preços ensejará aplicação das penalidades estabelecidas no Edital**.

10.1.1. As sanções também se aplicam aos integrantes do cadastro de reserva no registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente após terem assinado a ata.

10.2. É da competência do órgão gerenciador a aplicação das penalidades decorrentes do descumprimento do pactuado nesta ata de registro de preço (art. 7º, XIV, do Decreto 11.462/2023), exceto nas hipóteses em que o descumprimento disser respeito às contratações dos órgãos ou entidades participantes, caso no qual caberá ao respectivo órgão participante a aplicação da penalidade (art. 8º, IX, do Decreto 11.462/2023).

10.3. O órgão ou entidade participante deverá comunicar ao órgão gerenciador qualquer das ocorrências previstas no subitem 9.1, dada a necessidade de instauração de procedimento para cancelamento do registro do fornecedor.

11. CONDIÇÕES GERAIS

11.1. As condições gerais de execução do objeto, tais como os prazos para entrega e recebimento, as obrigações da Administração e do fornecedor registrado, penalidades e demais condições do ajuste, encontram-se definidos no Termo de Referência, Anexo ao Edital.

11.2. No caso de adjudicação por preço global de grupo de itens, só será admitida a contratação de parte de itens do grupo se houver prévia pesquisa de mercado e demonstração de sua vantagem para o órgão ou a entidade.

Para firmeza e validade do pactuado, a presente Ata, depois de lida e achada em ordem, vai assinada pelas partes.

Diretor-Geral do Tribunal Regional Federal da 6ª Região
Tribunal Regional Federal da 6ª Região em Minas Gerais
- assinado eletronicamente -

Representante do Licitante
- assinado eletronicamente -

Anexo

Cadastro de Reserva

Seguindo a ordem de classificação, segue relação de fornecedores que aceitaram cotar os itens com preços iguais ao adjudicatário:

Item do TR	**Fornecedor** (razão social, CNPJ/MF, endereço, contatos, representante)							
-	**Especificação**	**Marca** (se exigida no edital)	**Modelo** (se exigido no edital)	**Unidade**	**Quantidade Máxima**	**Quantidade Mínima**	**Valor Unitário**	**Prazo de garantia ou validade**

Seguindo a ordem de classificação, segue relação de fornecedores que mantiveram sua proposta original:

Item do TR	**Fornecedor** (razão social, CNPJ/MF, endereço, contatos, representante)

-	**Especificação**	**Marca** (se exigida no edital)	**Modelo** (se exigido no edital)	**Unidade**	**Quantidade Máxima**	**Quantidade Mínima**	**Valor Unitário**	**Prazo de garantia ou validade**

Documento assinado eletronicamente por **Marcela Junia Emidio do Carmo**, **Supervisor(a) de Seção**, em 11/02/2025, às 15:52, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.trf6.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1113306** e o código CRC **511BDC56**.

PODER JUDICIÁRIO
TRIBUNAL REGIONAL FEDERAL DA 6ª REGIÃO
Seção de Contratos

CONTRATO MINUTA 1113773

PROCESSO SEI Nº 0006130-19.2024.4.06.8000

Ata de Registro de Preços nº __/2024 - TRF6 - Pregão Eletrônico nº 90017/2024

CONTRATO Nº __/_____ DE SOLUÇÃO DE SEGURANÇA DE TIC COM A FINALIDADE DE ATENDER ÀS NECESSIDADES DE FUNCIONAMENTO DOS SISTEMAS DO TRIBUNAL REGIONAL FEDERAL DA 6ª REGIÃO, QUE CELEBRAM ENTRE SI O TRIBUNAL REGIONAL FEDERAL DA SEXTA REGIÃO E A **EMPRESA _____.**

MINUTA

A **UNIÃO**, por meio do **TRIBUNAL REGIONAL FEDERAL DA SEXTA REGIÃO**, inscrita no CNPJ sob o n° 47.784.477/0001-79, com sede na Avenida Álvares Cabral, 1805, Bairro Santo Agostinho, Belo Horizonte/MG, neste ato representada pelo Sr. Diretor-Geral, Dr. Jânio Mady dos Santos, por delegação da Portaria TRF6-Presi 103 (0102883), de 21/11/2022, doravante denominado CONTRATANTE e, de outro lado, a empresa _____, CNPJ nº _____, com sede _____, que apresentou os documentos exigidos por lei, neste ato representada por _____, já qualificado nos autos do processo, daqui por diante designada CONTRATADA, que têm, entre si, justo e avençado, e celebram o presente contrato, por força do presente instrumento e de conformidade com a Resolução CNJ 468/2022, com as normas constantes na Lei 14.133/2021 e no Decreto 11.462/2023, mediante as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA - DO OBJETO

1.1 Esta contratação tem por objeto aquisição de Solução de Segurança de TIC, incluindo o fornecimento de *Appliances de NGFW* e respectivos licenciamentos, o licenciamento de *Appliance* Virtual de Web Application Firewall e o licenciamento de Serviço de Segurança de Borda (*Security Service Edge - SSE*), incluindo os serviços de instalação, suporte técnico e treinamento, por um período de 60 (sessenta) meses, para atendimento das necessidades de funcionamento dos sistemas do Tribunal Regional Federal da Sexta Região, conforme condições, quantidades e exigências estabelecidas no Termo de Referência id. _____, na Ata de Registro de Preços nº ____/_____ - TRF6 e especificações abaixo:

(Inserir quadro referente aos itens contratados, conforme item 1.2.1 do Termo de Referência)

1.2. Vinculam esta contratação, independentemente de transcrição:

a. O Termo de Referência (id. ....);

b. O Edital de Licitação (id. ...) ;

c. A Ata de Registro de Preços (id. ....) ;

d. Eventuais anexos dos documentos supracitados.

CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO: O prazo de vigência da contratação é de 60 (sessenta) meses contados da assinatura do contrato, prorrogável por igual período, na forma do item **1.4** do Termo de Referência e dos artigos 106 e 107 da Lei nº 14.133, de 2021.

2.1. O término da vigência contratual será fixado por apostilamento, após o recebimento definitivo do seu objeto, contando-se 60 (sessenta) meses a partir deste marco, que deverá ser certificado no processo pelo gestor designado.

2.2. O prazo de entrega dos bens é de 90 (noventa) dias corridos, a contar da emissão da Ordem de Fornecimento, na forma dos itens **6.8.2 e 11.6** do Termo de Referência.

2.3. O objeto deverá ser entregue às expensas do fornecedor, sem custo adicional para o contratante, incluindo todos os acessórios de hardware e software necessários à perfeita instalação e funcionamento, devendo ser entregue em conformidade com as disposições previstas no item **11.6** do Termo de Referência.

CLÁUSULA TERCEIRA - PREÇO: A Contratada receberá do contratante o valor total de R$_____ (_____), em conformidade com os valores unitários registrados na Ata de Registro de Preços nº ____/_____- TRF6 (id. ...).

3.1. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

CLÁUSULA QUARTA - DOTAÇÃO ORÇAMENTÁRIA: As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União deste exercício, na dotação abaixo discriminada:

(Inserir dotações orçamentárias dos itens contratados. Para o TRF6: referenciadas na informação id. 1031674)

Ação Orçamentária:	**4257** - Julgamento de Causas na Justiça Federal
Plano Orçamentário:	**- TISI**: Capacitação de Servidores Efetivos e Comissionados das Unidades de Tecnologia da Informação e Segurança da Informação do Poder Judiciário (itens 05, 09 e 13); **- 0010**: Ações de Informática (demais itens).

Parágrafo Único: Será emitida nota de empenho à conta da dotação orçamentária especificada nesta cláusula para fazer frente às despesas oriundas desta contratação. A dotação relativa aos exercícios financeiros subsequentes, se for o caso, será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes.

CLÁUSULA QUINTA – RECEBIMENTO, LIQUIDAÇÃO E PAGAMENTO: as premissas relativas ao pagamento das obrigações oriundas deste contrato são aquelas previstas no item **13. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO** do Termo de Referência.

5.1. A emissão da Nota Fiscal/Fatura será precedida do recebimento definitivo do objeto da contratação, conforme disposto neste instrumento e/ou Termo de Referência.

5.2. Quando houver glosa parcial do objeto, o contratante deverá comunicar a empresa para que emita a nota fiscal ou fatura com o valor exato dimensionado.

CLÁUSULA SEXTA - MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS: Para correta execução dos serviços a CONTRATADA deverá observar as disposições constantes nos itens **1. OBJETO, 5. DETALHAMENTO DOS LOTES E ITENS**, **6. REQUISITOS DA CONTRATAÇÃO, 7. CONTROLE DE ACESSO E VALIDAÇÃO, 8. DA PROPRIEDADE INTELECTUAL E DIREITO AUTORAL, 9. NÍVEIS DE SERVIÇO, 11. MODELO DE EXECUÇÃO DO OBJETO, 12. MODELO DE GESTÃO DO CONTRATO e 13. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO** do Termo de Referência.

CLÁUSULA SÉTIMA – SUBCONTRATAÇÃO: É permitida a subcontratação parcial do objeto contratual, nos termos do **item 9.10** do Termo de Referência.

CLÁUSULA OITAVA - OBRIGAÇÕES DA CONTRATANTE: são obrigações da CONTRATANTE, sem prejuízo daquelas previstas notadamente no item **14. OBRIGAÇÕES DA CONTRATANTE** Termo de Referência bem como neste instrumento.

CLÁUSULA NONA – OBRIGAÇÕES DA CONTRATADA: São obrigações da CONTRATADA, além daquelas previstas neste instrumento e principalmente no item **15. OBRIGAÇÕES DA CONTRATADA** do Termo de Referência.

CLÁUSULA DEZ - REAJUSTE: Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, em ___/___/_____.

10.1. Após o interregno de um ano, os preços iniciais poderão ser reajustados, mediante a aplicação, pelo contratante, do índice IPCA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

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

10.3. No caso de atraso ou não divulgação do índice de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.

10.4. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.

10.5. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

10.6. O reajuste será realizado por apostilamento.

CLÁUSULA ONZE - DA GARANTIA DE EXECUÇÃO: Haverá exigência de garantia de execução do objeto, prevista nos artigos 96 e seguintes da Lei nº 14.133/21, nos termos do item **10. GARANTIA DA CONTRATAÇÃO** do Termo de Referência.

11.1. O contratado apresentará comprovante de prestação de garantia, podendo optar por caução em dinheiro, pela fiança bancária, em valor correspondente a correspondente a 5% (cinco por cento) do valor total do contrato.

11.2. Caso utilizada a modalidade de seguro-garantia, a apólice deverá ter validade durante a vigência do contrato e por mais 90 (noventa) dias após término deste prazo de vigência, permanecendo em vigor mesmo que o

contratado não pague o prêmio nas datas convencionadas.

11.3. A garantia nas modalidades caução e fiança bancária deverá ser prestada em até 15 dias após a assinatura do contrato.

11.4. No caso de seguro-garantia, sua apresentação deverá ocorrer, no máximo, até a data de assinatura do contrato;

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

11.6. Será permitida a substituição da apólice de seguro-garantia na data de renovação ou de aniversário, desde que mantidas as condições e coberturas da apólice vigente e nenhum período fique descoberto, ressalvado o disposto no item 11.5. deste contrato.

11.7. Na hipótese de suspensão do contrato por ordem ou inadimplemento da Administração, o contratado ficará desobrigado de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pela Administração.

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

a) prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

b) multas moratórias e punitivas aplicadas pela Administração à contratada; e

c) obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pelo contratado, quando couber.

11.9. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item 11.8. deste contrato, observada a legislação que rege a matéria.

11.10. A garantia em dinheiro deverá ser efetuada em favor do contratante, em conta específica na Caixa Econômica Federal, com correção monetária.

11.11. No caso de garantia na modalidade de fiança bancária, deverá ser emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil, e deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

11.12. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.

11.13. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, o Contratado obriga-se a fazer a respectiva reposição no prazo máximo de 10 (dez) dias úteis, contados da data em que for notificada.

11.14. O emitente da garantia ofertada pelo contratado deverá ser notificado pelo contratante quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais (art. 137, § 4º, da Lei n.º 14.133, de 2021).

11.15. Caso se trate da modalidade seguro-garantia, ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos do art. 20 da Circular Susep n° 662, de 11 de abril de 2022.

11.16. Extinguir-se-á a garantia com a restituição da apólice, carta fiança ou autorização para a liberação de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do contratante, mediante termo circunstanciado, de que o contratado cumpriu todas as cláusulas do contrato;

11.17. A garantia somente será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da Administração e, quando em dinheiro, será atualizada monetariamente.

11.18. O garantidor não é parte para figurar em processo administrativo instaurado pelo contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada.

11.19. O contratado autoriza o contratante a reter, a qualquer tempo, a garantia, na forma prevista neste Contrato.

CLÁUSULA DOZE – DAS SANÇÕES: As sanções relacionadas à execução do contrato e condições para aplicação das penalidades são as seguintes, observados os preceitos contidos no item **16. SANÇÕES ADMINISTRATIVAS** do Termo de Referência:

I - Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o contratado que:

a) der causa à inexecução parcial do contrato;

b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;
c) der causa à inexecução total do contrato;
d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;
f) praticar ato fraudulento na execução do contrato;
g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

II - Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:

a) Advertência, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei nº 14.133, de 2021);
b) Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas "b", "c" e "d" do subitem acima deste Contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);
c) Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas "e", "f", "g" e "h" do subitem acima deste Contrato, bem como nas alíneas "b", "c" e "d", que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 2021);

d) Multa.

§ 1º A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante (art. 156, §9º, da Lei nº 14.133, de 2021).
§ 2º Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133, de 2021).
§ 3º Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157, da Lei nº 14.133, de 2021).
§ 4º 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 poderá ser descontada da garantia, se for o caso, ou cobrada judicialmente (art. 156, §8º, da Lei nº 14.133, de 2021).
§ 5º Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de **30 (trinta) dias**, a contar da data do recebimento da comunicação enviada pela autoridade competente.
§ 6º A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.
§ 7º Na aplicação das sanções serão considerados (art. 156, §1º, da Lei nº 14.133, de 2021):

a) a natureza e a gravidade da infração cometida;
b) as peculiaridades do caso concreto;
c) as circunstâncias agravantes ou atenuantes;
d) os danos que dela provierem para o Contratante;
e) a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

§8º Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013,

serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159 da Lei nº 14.133, de 2021).

§9º A personalidade jurídica da contratada poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com a contratada, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160 da Lei nº 14.133, de 2021).

§10 Os contratantes deverão, no prazo máximo **15 (quinze)** dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal. (Art. 161 da Lei nº 14.133, de 2021).

§11 As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação, na forma do art. 163 da Lei nº 14.133/21.

§12 Os débitos da contratada para com a Administração contratantes, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que a contratada possua com o mesmo órgão dos contratantes, na forma da legislação aplicável.

§13 Nos termos da Lei n. 14.133/2021, o órgão gerenciador e os participantes poderão aplicar as penalidades descritas neste termo de referência, observado o regular processo administrativo, assegurado o contraditório e a ampla defesa.

CLÁUSULA TREZE - PROTEÇÃO DE DADOS: Integra a este contrato, as disposições referentes à Lei Geral de Proteção de Dados, nos termos do item **17. DA PROTEÇÃO DE DADOS**, do Termo de Referência anexo a este contrato.

CLÁUSULA QUATORZE – ALTERAÇÕES: Eventuais alterações contratuais reger-se-ão pela disciplina dos artigos 124 e seguintes da Lei nº 14.133, de 2021.

14.1. O contratado é obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

14.2. As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia aprovação da consultoria jurídica do contratante, salvo nos casos de justificada necessidade de antecipação de seus efeitos, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 1 (um) mês (art. 132 da Lei nº 14.133, de 2021).

14.3. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de 2021.

CLÁUSULA QUINZE – DA EXTINÇÃO CONTRATUAL: O contrato será extinto com o decurso do prazo previsto na cláusula segunda deste instrumento.

15.1. O contrato poderá ser extinto antes do prazo nele fixado, sem ônus para o contratante, quando esta não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

15.2. O contrato poderá ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

15.2.1. Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei.

15.2.2. A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a extinção se não restringir sua capacidade de concluir o contrato.

15.2.2.1. Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

15.3. O termo de extinção, sempre que possível, será precedido:

a. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

b. Relação dos pagamentos já efetuados e ainda devidos;

c. Indenizações e multas.

15.4. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório (art. 131, caput, da Lei n.º 14.133, de 2021).

15.5. O contrato poderá ser extinto caso se constate que o contratado mantém vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que tenha desempenhado função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau (art. 14, inciso IV, da Lei n.º 14.133, de 2021).

CLÁUSULA DEZESSEIS – DOS CASOS OMISSOS: Os casos omissos serão decididos pelo contratante, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

CLÁUSULA DEZESSETE – PUBLICAÇÃO : Incumbirá ao contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo sítio oficial na Internet, em atenção ao art. 91, caput, da Lei n.º 14.133, de 2021.

CLÁUSULA DEZOITO – FORO: Fica eleito o Foro da Justiça Federal- Seção Judiciária do Estado de Minas Gerais para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não puderem ser compostos pela conciliação, conforme art. 92, §1º, da Lei nº 14.133/21.

Jânio Mady dos Santos

DIRETOR-GERAL

TRIBUNAL REGIONAL FEDERAL DA 6ª REGIÃO

Representante

RAZÃO SOCIAL DA EMPRESA

- Assinado digitalmente -

DOCUMENTO ASSINADO PARA POSSIBILITAR A VISUALIZAÇÃO POR OUTROS SETORES

Documento assinado eletronicamente por **Bruno Guimaraes Valadares**, **Supervisor(a) de Seção**, em 11/02/2025, às 17:50, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.trf6.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1113773** e o código CRC **EAA0ACE8**.