006718/25-00.082

PODER JUDICIÁRIO
SUPERIOR TRIBUNAL MILITAR
PRSTM/SECSTM/DITIN/COTEC

TERMO DE REFERÊNCIA - SERVIÇOS COMUNS - LICITAÇÃO

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

Objeto da contratação

1.1. Contratação de **empresa especializada em segurança cibernética para prestação de Serviço Gerenciado de Segurança da Informação, composta por equipamento para proteção de perímetro do tipo NGFW com SD-WAN, suporte e garantia pelo período de 60 meses, pelo Sistema de Registro de Preços**, conforme condições e exigências estabelecidas neste instrumento.

1.1.1. **Justificativa para o não parcelamento do objeto:**

A regra geral na administração pública é o parcelamento do objeto, visando ampliar a competitividade. No entanto, para a presente contratação, o parcelamento se mostra tecnicamente inviável e antieconômico, representando um risco inaceitável para a segurança e a operação do STM. O objeto contratual não é uma soma de partes independentes, mas sim um **serviço único e indivisível de Segurança Gerenciada**. A eficácia da solução depende da sinergia total entre o hardware (NGFW), o software (licenças de segurança), o serviço de monitoramento (SOC/NOC) e o suporte especializado (profissional dedicado). A tentativa de parcelar este objeto — por exemplo, licitando os equipamentos com uma empresa e o serviço de gerenciamento com outra — resultaria em graves prejuízos técnicos e de gestão, como a diluição de responsabilidade em caso de incidentes e a inviabilidade de aplicação do Acordo de Nível de Serviço (SLA). Conclui-se, portanto, que a natureza integrada do serviço exige um fornecedor único que seja totalmente responsável pela solução de ponta a ponta. A contratação do objeto em um **grupo único** é a única forma de garantir a responsabilidade, a coesão técnica e a eficácia do serviço de segurança.

grupo	Item	Descrição dos serviços	CATSER	Unidade de Medida	Quantidade
1	1	Serviço composto por equipamento para proteção de perímetro do tipo NGFW com SD-WAN - Tipo I (Concentrador)	27073	Unidade	2
	2	Serviço composto por equipamento para proteção de perímetro do tipo NGFW com SD-WAN - Tipo II (Unidades Remotas)	27073	Unidade	1
	3	Serviço composto por equipamento para proteção de perímetro do tipo NGFW com SD-WAN - Tipo III (Unidades Remotas)	27073	Unidade	3
	4	Serviço composto por equipamento para proteção de perímetro do tipo NGFW com SD-WAN - Tipo IV (Unidades Remotas)	27073	Unidade	12
	5	Serviço composto por Gerência centralizada, logs, eventos e relatórios para equipamentos de proteção de perímetro com SD-WAN.	27073	Unidade	1

1.2. A parcela do objeto desta contratação que envolve bens de consumo não se enquadra como sendo de bem de luxo, conforme Ato Normativo PRSTM nº 702, de 2024 (3564810).

1.3. Os serviços objeto desta contratação são caracterizados como **comuns**, com respaldo nesta justificativa:

O objeto da contratação, embora tecnicamente complexo, enquadra-se na definição de serviço comum, nos termos da Lei nº 14.133/2021. Seus padrões de desempenho e qualidade podem ser objetivamente definidos por meio de especificações usuais de mercado, conforme detalhado exaustivamente no Estudo Técnico Preliminar e consolidado neste Termo de Referência. A existência de um mercado competitivo, com múltiplos fornecedores capazes de atender aos requisitos, reforça essa caracterização, tornando a modalidade

Pregão Eletrônico a mais adequada e eficiente para a seleção da proposta mais vantajosa para a Administração.

1.4. A contratação dar-se-á *por instrumento próprio, cuja minuta constitui ANEXO do Edital.*

1.5. Como condição à assinatura do contrato ou à emissão de instrumento equivalente, será exigida a comprovação:

1.5.1. da regularidade fiscal do Licitante vencedor, conforme previsto nos requisitos de habilitação (art. 90, § 4º, da Lei nº 14.133, de 2021);

1.5.2. de inexistência de sanção que impeça a contratação no SICAF, no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS), no Cadastro Nacional de Empresas Punidas (CNEP), no Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça, e no Cadastro de Licitantes Inidôneos, mantido pelo Tribunal de Contas da União (art. 90, § 4º, da Lei nº 14.133, de 2021);

1.5.2.1. a consulta ao Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa será realizada em nome do licitante vencedor e também de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei nº 8.429, de 1992;

1.5.3. de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a certidão negativa ou positiva com efeitos de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943 (art. 90, § 4º, da Lei nº 14.133, de 2021); e

1.5.4. de inexistência de registro no Cadastro Informativo de créditos não quitados no setor público federal (CADIN) (art. 6º-A da Lei nº 10.522, de 2021).

1.6. Na hipótese de o Licitante vencedor não cumprir as condições do subitem 1.5., será facultado à Administração convocar os licitantes remanescentes, na ordem de classificação, para celebração da contratação, conforme as regras do art. 90 da Lei nº 14.133, de 2021;

1.7. O Aceite da Nota de Empenho, emitida ao fornecedor adjudicado, implica, se esse instrumento for utilizado para substituir o instrumento "contrato", o reconhecimento de que:

1.7.1. referida Nota está substituindo o contrato, aplicando-se à relação de negócios ali estabelecida as disposições da Lei nº 14.133, de 2021;

1.7.2. a contratada se vincula à sua proposta e às previsões contidas no Edital, neste Termo de Referência e em eventuais anexos de ambos;

1.7.3. a contratada reconhece que as hipóteses de rescisão são aquelas previstas nos artigos 137 e 138 da Lei nº 14.133, de 2021, e reconhece os direitos da Administração previstos nos artigos 137 a 139 desta Lei.

1.8. O **Representante Legal do Licitante vencedor,** após a adjudicação e a homologação, **deverá obrigatoriamente** se cadastrar, **no prazo de três dias úteis**, prorrogável por igual período, no acesso externo do Sistema Eletrônico de Informações (SEI) no endereço:

https://sei.stm.jus.br/controlador_externo.php?acao=usuario_externo_logar&acao_origem=usuario_externo_gerar_senha&id_orgao_acesso_externo=0

1.8.1. A não obtenção do cadastro como usuário externo, bem como eventual erro de transmissão ou recepção de dados não imputáveis a falhas do SEI-JMU ou de sistema integrado, não servirão de escusa para o descumprimento de obrigações e prazos.

1.8.2. As pessoas jurídicas ficam obrigadas a solicitar a inativação de usuários externos que não pertençam mais aos seus quadros, sob pena de responzabilização pelo uso indevido do Sistema.

1.8.3. O uso indevido do Sistema será passível de apuração de responsabilidade nas esferas administrativa, civil e penal.

1.8.4. Após o cadastro no SEI as respectivas unidades poderão disponibilizar o acesso para o Licitante assinar os documentos, nos prazos contratualmente estipulados.

1.8.5. O referido cadastro possibilitará ao fornecedor/contratada realizar o **Peticionamento eletrônico, regulamentado pelo Ato Normativo STM nº 430, de 2020 (https://www2.stm.jus.br/sislegis/index.php/ctrl_publico_pdf/visualizar/27452-ATN-000430_28-07-2020_STM_1.pdf), para o envio dos documentos** necessários durante todo o período da contratação, tais como: documentos pessoais do responsável legal, procurações, contratos sociais, ofícios diversos, pedidos de repactuação/reajuste, notas fiscais, faturas e comprovantes de pagamentos de encargos, defesa prévia e recursos referentes a penalidades contratuais, entre outros.

1.8.5.1. De acordo com o artigo 14 do referido Ato, não será admitido intimar ou protocolar documentos por meio físico, exceto quando houver inviabilidade técnica ou indisponibilidade do meio eletrônico cujo prolongamento cause dano relevante à celeridade ou à instrução do processo, ou quando houver exceção prevista em instrumento normativo próprio.

1.9. A Administração, desde que, se for o caso, apresentado seguro-garantia, encaminhará e-mail com o link do contrato a ser assinado, o que deverá ocorrer no prazo máximo de três dias úteis, prorrogáveis por mais três a pedido do Fornecedor, devidamente justificado, e autorizado pela Administração, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas no Edital.

Vigência da contratação

1.10. O prazo de vigência da contratação é de 60 (sessenta) meses, contados do primeiro dia útil subsequente à publicação do contrato no Portal Nacional de Contratações Públicas (PNCP), prorrogável por até 10 (dez) anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021, devendo essa publicação acontecer no prazo máximo de 20 (vinte) dias úteis, a partir de sua assinatura.

1.10.1. O serviço é enquadrado como **continuado**, tendo em vista que a necessidade de proteger os sistemas e as informações da Justiça Militar da União é permanente, essencial e indispensável ao funcionamento diário da instituição, não sendo um projeto com início, meio e fim. A interrupção deste serviço resultaria em impacto catastrófico e imediato sobre todas as atividades do STM e das Auditorias. A vigência plurianual de 60 meses é mais vantajosa para a Administração, considerando os seguintes fatores extraídos do Estudo Técnico Preliminar (SEI 4382819):

1.10.1.1. **Viabilidade Econômica:** A contratação envolve um investimento inicial significativo por parte da CONTRATADA no fornecimento de 18 equipamentos de hardware de alto valor. Um prazo de vigência de 60 meses permite a amortização desse investimento ao longo do tempo, resultando em um valor de mensalidade consideravelmente menor para o STM, ao passo que um prazo mais curto tornaria o valor do serviço proibitivo.

1.10.1.2. **Estabilidade e Maturidade do Serviço:** Um contrato de longo prazo é fundamental para a maturação do serviço prestado, pois permite que a equipe da CONTRATADA, em especial o profissional dedicado, desenvolva um profundo conhecimento sobre o ambiente e as necessidades específicas do STM, resultando em um serviço mais estável e proativo.

1.10.1.3. **Redução de Custos Administrativos:** A celebração de um contrato de 60 meses evita a necessidade de realizar novos e complexos processos licitatórios a cada 12 ou 24 meses, reduzindo significativamente a carga de trabalho das áreas administrativa e técnica do STM.

1.10.2. A prorrogação de que trata este item é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com a contratada, atentando, ainda, para o cumprimento dos seguintes requisitos:

1.10.2.1. Estar formalmente demonstrado no processo que a forma de prestação dos serviços tem natureza continuada;

1.10.2.2. Seja juntado relatório que discorra sobre a execução do contrato, com informações de que os serviços tenham sido prestados regularmente;

1.10.2.3. Seja juntada justificativa e motivo, por escrito, de que a Administração mantém interesse na realização do serviço;

1.10.2.4. Haja manifestação expressa da contratada informando o interesse na prorrogação; e

1.10.2.4.1. A fiscalização, até 180 (cento e oitenta) dias do término da vigência contratual, deverá expedir comunicado à contratada para que esta manifeste, no prazo de 10 (dez) dias, o seu interesse na prorrogação.

1.10.2.5. Seja comprovado que a contratada mantém as condições iniciais de habilitação.

1.11. A contratada não tem direito subjetivo à prorrogação contratual.

1.12. A prorrogação do contrato deverá ser promovida mediante celebração de termo aditivo.

1.13. Nas eventuais prorrogações contratuais, os custos não renováveis já pagos ou amortizados ao longo do primeiro período de vigência da contratação deverão ser reduzidos ou eliminados como condição para a prorrogação.

1.14. O contrato não poderá ser prorrogado quando a contratada tiver sido penalizada nas sanções de declaração de inidoneidade ou impedimento de licitar e contratar com o poder público, observadas as abrangências de aplicação.

1.15. O contrato não poderá ser prorrogado quando for identificado registro no CADIN em nome da contratada (art. 6º-A da Lei nº 10.522, de 2002).

1.15.1. O Contratante poderá, entendendo conveniente, conceder prazo para regularização do registro no CADIN, antes de *descartar a prorrogação do contrato como o instrumento apto a atender a necessidade pública.*

1.15.2. Caso a contratada regularize o registro no CADIN depois que o Contratante já iniciou o planejamento para atendimento da necessidade pública por outros meios, a Administração poderá, entendendo conveniente, reconsiderar sua decisão inicial, optando pela renovação, desde que cumpridos todos os outros requisitos para a prorrogação;

1.15.3. Havendo fundamentado risco de prejuízo com a não prorrogação do contrato, como, exemplificativamente, a interrupção do serviço contínuo, a Administração poderá, desde que demonstrado que a renovação é a forma mais adequada de evitá-lo, prorrogar a contratação, a despeito da manutenção do registro no CADIN, pelo período necessário para a conclusão da licitação que selecionará o próximo prestador de serviços.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. A Fundamentação da Contratação e de seus quantitativos é a seguinte:

A presente contratação fundamenta-se na necessidade crítica de modernizar e fortalecer a segurança cibernética da Justiça Militar da União (JMU), garantindo a proteção de seus ativos de informação e a continuidade de seus serviços essenciais. O cenário de evolução tecnológica e a crescente complexidade dos crimes virtuais impõem a atualização contínua das ferramentas de segurança para proteger a JMU de prejuízos incalculáveis e para assegurar a estabilidade dos sistemas judiciais e administrativos.

A demanda está em plena conformidade com os instrumentos estratégicos do Poder Judiciário, como a Estratégia Nacional de Tecnologia da Informação e Comunicação (ENTIC-JUD - Resolução CNJ nº 370/2021) e a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ - Resolução CNJ nº 396/2021). Internamente, alinha-se aos objetivos do Planejamento Estratégico da JMU (PEJMU 2021-2026) e atende diretamente às metas e ações previstas no Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC 2025-2026), que identifica "Ataques cibernéticos" como uma ameaça externa e estabelece "Aprimorar a Segurança da Informação e a Gestão de Dados" como um objetivo estratégico (OE6).

Item	Descrição do Serviço/Equipamento	Unidade	Quantidade	Justificativa da Quantidade
1	Serviço composto por equipamento NGFW com SD-WAN Tipo I (Concentrador)	Unidade	2	Destinados ao Data Center da Sede do STM, para operar em um cluster de Alta Disponibilidade (Ativo/Passivo), garantindo redundância e continuidade em caso de falha de um dos equipamentos.
2	Serviço composto por equipamento NGFW com SD-WAN Tipo II (Unidades Remotas)	Unidade	1	Para atender à auditoria remota de maior porte da JMU (local de backup), com maior número de usuários e volume de tráfego, exigindo interfaces de alta velocidade.

Item	Descrição do Serviço/Equipamento	Unidade	Quantidade	Justificativa da Quantidade
3	Serviço composto por equipamento NGFW com SD-WAN Tipo III (Unidades Remotas)	Unidade	3	Para atender às auditorias remotas de médio porte (Rio de Janeiro, São Paulo e Brasília), dimensionadas conforme a estrutura e necessidade dessas localidades.
4	Serviço composto por equipamento NGFW com SD-WAN Tipo IV (Unidades Remotas)	Unidade	12	Para atender às auditorias remotas de menor porte, garantindo o mesmo nível de segurança com um equipamento de performance e custo adequados à sua demanda.
5	Serviço composto por Gerência centralizada, logs, eventos e relatórios	Unidade	1	Um único serviço de gerenciamento centralizado é necessário para administrar, monitorar e correlacionar os eventos de todos os 18 equipamentos (2+1+3+12), garantindo visibilidade unificada e consistência nas políticas.

2.2. O objeto da contratação está previsto no Plano de Contratações Anual (PCA) **2025**, conforme publicação no sítio eletrônico da Justiça Militar da União.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO

3.1. A solução a ser contratada consiste na prestação de um **Serviço Gerenciado de Segurança da Informação (MSS - Managed Security Service)**, de natureza continuada, pelo período de 60 (sessenta) meses. Trata-se de um serviço completo e contínuo, no qual a empresa CONTRATADA será responsável por todo o ciclo de vida da segurança de perímetro da Justiça Militar da União.

3.2. A solução abrange os seguintes componentes principais:

3.2.1. **Fornecimento de Equipamentos:** A CONTRATADA fornecerá 18 (dezoito) equipamentos de proteção de perímetro do tipo NGFW com funcionalidade de SD-WAN, adequados para cada localidade da JMU (Sede e Auditorias), em regime de comodato ou como parte integrante do serviço.

3.2.2. **Licenciamento de Software**: Fornecimento de todas as licenças de software (subscrições) necessárias para a operação plena das funcionalidades de segurança avançada, como IPS, Filtro de Conteúdo, Antimalware, Sandboxing e SD-WAN.

3.2.3. **Implantação e Gestão Contínua**: A CONTRATADA será responsável pela implantação, configuração e otimização contínua da solução.

3.2.3. **Monitoramento Proativo (SOC/NOC):** A solução inclui o monitoramento proativo de segurança e desempenho, 24 horas por dia, 7 dias por semana, por meio de um Centro de Operações de Segurança (SOC) e de Rede (NOC) da CONTRATADA.

3.2.4. **Suporte Especializado Dedicado**: Alocação de 01 (um) profissional sênior, certificado e com dedicação exclusiva ao ambiente do STM, para atuar como ponto focal técnico, garantindo agilidade e expertise no suporte avançado e na gestão estratégica da solução.

3.3. O ciclo de vida do objeto, considerando o prazo de 60 meses, inclui a constante atualização tecnológica (updates de software e assinaturas), a manutenção preventiva e corretiva dos equipamentos e, ao final do contrato, a remoção de todos os equipamentos pela CONTRATADA e a transferência de todo o conhecimento e dados de configuração para o STM, garantindo sua independência tecnológica.

3.4. **Justificativa para Adoção do Sistema de Registro de Preços (SRP):**

3.4.1. A licitação será processada por meio do Sistema de Registro de Preços (SRP) para gerar uma Ata de Registro de Preços com validade de 12 meses. A adoção do SRP é a estratégia mais vantajosa, pois permite uma implementação em fases, otimizando a logística e o planejamento. A execução seguirá uma ordem de prioridade, iniciando-se pela infraestrutura crítica na Sede do STM (Fase 1) e, subsequentemente, implantando os equipamentos nas 16 Auditorias remotas sob demanda (Fases Subsequentes). Esta abordagem proporciona flexibilidade para coordenar a logística complexa em múltiplas unidades federativas e alinha os desembolsos orçamentários ao cronograma de implantação física.

3.5. **Justificativa para Permissão de Consórcio e Subcontratação:**

3.5.1. **Consórcio**: Será permitida a participação de empresas em consórcio como forma de ampliar a competitividade e permitir a união de expertises, desde que atendidas todas as exigências de qualificação do edital.

3.6. **Subcontratação:**

3.6.1. Será permitida a subcontratação de partes do serviço (como o monitoramento de primeiro nível pelo SOC/NOC), desde que a CONTRATADA permaneça como única e total responsável perante o STM pelo cumprimento do contrato e do SLA. Fica **expressamente vedada a subcontratação do profissional sênior dedicado**, por ser este o núcleo da expertise e do relacionamento técnico com o STM. Toda subcontratação dependerá de aprovação prévia do STM.

3.7. **Justificativa para Vedação à Participação de Pessoas Físicas**: A participação de pessoas físicas é vedada devido à natureza e complexidade do objeto. A contratação exige uma estrutura empresarial robusta, capaz de:

3.7.1. Fornecer e garantir 18 equipamentos de hardware de alto valor em todo o território nacional.

3.7.2. Manter um Centro de Operações de Segurança e Rede (SOC/NOC) funcionando em regime 24x7x365 para monitoramento contínuo.

3.7.3. Disponibilizar uma equipe de suporte com múltiplos níveis de especialização e garantir o cumprimento de um Acordo de Nível de Serviço (SLA) rigoroso.

3.7.4. Alocar um profissional sênior de forma dedicada e exclusiva, com capacidade de prover substituto em caso de ausência.

3.7.5. Tais requisitos ultrapassam a capacidade de um prestador de serviço individual, sendo indispensável a participação de pessoas jurídicas com estrutura e capacidade operacional compatíveis.

4. REQUISITOS DA CONTRATAÇÃO

Sustentabilidade

Conforme assinalado no Documento de Oficialização da Demanda (DOD), a presente aquisição não possui requisitos pré-definidos na Política de Sustentabilidade/Acessibilidade da Assessoria de Gestão Estratégica. Embora a presente contratação se caracterize majoritariamente como **prestação de serviço de natureza intelectual e contínua**, a solução a ser implantada envolve o fornecimento de equipamentos de hardware. Desta forma, em observância ao princípio do desenvolvimento nacional sustentável, expresso no Art. 5º da Lei nº 14.133/2021 , e às boas práticas de contratações públicas, deverão ser atendidos os seguintes critérios de sustentabilidade:

4.1. Eficiência Energética dos Equipamentos:

4.1.1. A CONTRATADA deverá apresentar, como parte de sua proposta técnica, o datasheet ou documentação oficial do fabricante para cada tipo de equipamento ofertado, comprovando que os modelos possuem certificações de eficiência energética reconhecidas no mercado, como, por exemplo, o selo ENERGY STAR ou equivalente.

4.1.2. Justificativa: A exigência visa garantir que os equipamentos que operarão de forma ininterrupta (24x7) nas instalações da JMU possuam baixo consumo de energia, resultando em um impacto ambiental positivo pela redução da pegada de carbono e em economicidade para a Administração ao longo dos 60 meses de contrato.

4.2. Conformidade com Diretivas Ambientais:

4.2.1. Os equipamentos fornecidos deverão estar em conformidade com diretivas internacionais de restrição a substâncias perigosas, como a RoHS (Restriction of Hazardous Substances) ou equivalente. A comprovação poderá ser feita mediante declaração do fabricante ou informação contida na documentação técnica dos produtos.

4.2.2. Justificativa: Esta medida assegura que os equipamentos são fabricados com menor quantidade de materiais nocivos ao meio ambiente, como chumbo e mercúrio, facilitando seu descarte e reciclagem de forma mais segura ao final de sua vida útil.

4.3. Responsabilidade pelo Ciclo de Vida do Produto (Logística Reversa):

4.3.1. Ao término da vigência contratual, a CONTRATADA será a única e total responsável pela logística de desinstalação, remoção e descarte ambientalmente adequado de todos os seus equipamentos físicos das instalações da JMU.

4.3.2. O descarte deverá seguir as normas vigentes, em especial a Política Nacional de Resíduos Sólidos (Lei nº 12.305/2010), devendo a CONTRATADA apresentar, se solicitada pela fiscalização, comprovação da destinação correta dos resíduos eletrônicos.

4.3.3. Justificativa: Esta cláusula reforça que, sendo uma contratação de serviço, a responsabilidade pelo ciclo de vida completo do hardware, incluindo sua disposição final, é do prestador do serviço, eximindo a Administração de qualquer ônus ambiental e garantindo a aplicação do princípio da responsabilidade estendida do produtor/fornecedor.

4.4. Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os seguintes requisitos:

4.4.1. No caso de fornecimento de produtos ou equipamentos, se necessário a utilização de embalagens, a CONTRATADA deverá utilizar embalagens fabricadas com materiais que propiciem a reutilização ou reciclagem, com o menor volume possível, porém, com garantia de proteção durante o transporte e o armazenamento, conforme artigo 32 da Lei Federal nº 12.305/10, Instrução Normativa MPOG nº 1/2010 e Norma Brasileira ABNT NBR 16.182:2013.

4.4.2. A CONTRATADA deverá observar a Resolução CONAMA n.º 401/2008, para a aquisição de pilhas e baterias a serem utilizadas nos equipamentos, bens e materiais de sua responsabilidade, respeitando os limites de metais pesados, como chumbo, cádmio e mercúrio.

4.4.3. Em observação à Instrução Normativa MPOG nº 1/2010, sempre que aplicável, os materiais não devem conter substâncias perigosas em concentrações acima da recomendada na diretiva RoHS (Restrintion of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenil-polibromados (PBBs), éteres difenil-polibromados (PBDEs).

4.4.4. A CONTRATADA deverá observar, no que couber, as diretrizes do Plano de Logística Sustentável (PLS) do Superior Tribunal Militar durante a execução dos serviços.

4.4.5. Os equipamentos a serem fornecidos como parte do serviço deverão ser de tecnologia recente e priorizar a **eficiência energética**, visando um menor consumo de energia elétrica quando comparados a tecnologias mais antigas, o que representa um impacto ambiental positivo para a instituição.

4.4.6. Ao término do contrato, a CONTRATADA será a única responsável pela logística de desinstalação, remoção e **descarte ambientalmente adequado** de todos os seus equipamentos físicos das instalações da JMU. O descarte deverá seguir as normas vigentes, em especial a Política Nacional de Resíduos Sólidos (Lei nº 12.305/2010)

4.5. Na presente contratação **não será admitida a indicação de marca ou modelo específico**, a fim de preservar a ampla competitividade do certame.

Da exigência da amostra

4.6. A Administração, a seu critério e se julgar necessário, **poderá solicitar** ao licitante classificado provisoriamente em primeiro lugar a apresentação de amostra, que terá data, local e horário de sua realização divulgados por mensagem no sistema .

4.6.1. A análise da amostra poderá ser acompanhada por todos os interessados, não sendo permitidas, contudo, interferências verbais ou operacionais no decorrer dos procedimentos.

4.6.2. A Administração poderá solicitar informações adicionais referentes aos componentes e ao objeto, durante a análise da amostra.

4.7. Caso a Administração decida pela solicitação, será exigida amostra do seguinte item:

4.7.1**. Item 1 - Serviço composto por equipamento para proteção de perímetro do tipo NGFW com SD-WAN - Tipo I (Concentrador)**.

4.8. A amostra deverá ser entregue no endereço do Superior Tribunal Militar (Setor de Autarquias Sul, Praça dos Tribunais Superiores, Brasília/DF), no prazo máximo de **10 (dez) dias úteis** a contar da solicitação no sistema, sendo que a empresa assume total responsabilidade pelo envio e por eventual atraso na entrega .

4.9. É facultada prorrogação do prazo estabelecido, a partir de solicitação fundamentada no chat pelo interessado, antes de findo o prazo.

4.10. No caso de não haver entrega da amostra solicitada, ocorrer atraso na entrega sem justificativa aceita, ou havendo entrega de amostra fora das especificações previstas, a proposta será recusada.

4.11. Serão avaliados os seguintes aspectos e padrões mínimos de aceitabilidade em testes de bancada:

4.11.1. Aferição da capacidade de *throughput* de tráfego descriptografado pelo equipamento;

4.11.2. Aferição da capacidade de *throughput* de inspeção de tráfego SSL do equipamento;

4.11.3. Aferição das especificações técnicas de hardware (portas de comunicação, capacidade de processamento, memórias estática e volátil) do equipamento;

4.11.4. Verificação das capacidades do software embarcado no equipamento, conforme requisitos funcionais deste Termo de Referência.

4.12. Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

4.13. Se a amostra apresentada pelo primeiro classificado não for aceita, será analisada a aceitabilidade da proposta ou lance ofertado pelo segundo classificado, a quem também poderá ser solicitada a amostra e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes neste Termo de Referência.

4.14. Os exemplares colocados à disposição da Administração serão tratados como protótipos, podendo ser manuseados e desmontados pela equipe técnica responsável pela análise, não gerando direito a ressarcimento.

4.15. Após a divulgação do resultado final do certame, as amostras entregues deverão ser recolhidas pelos prestadores no prazo de 20 (vinte) dias, após o qual poderão ser descartadas pela Administração, sem direito a ressarcimento.

4.16. Os interessados deverão colocar à disposição da Administração todas as condições indispensáveis à realização de testes e fornecer, sem ônus, os manuais impressos em língua portuguesa, necessários ao seu perfeito manuseio, quando for o caso.

Subcontratação

4.17. É permitida a subcontratação parcial do objeto, até o limite de **30% (trinta por cento)** do valor do contrato, nas seguintes condições:

4.17.1. Poderão ser subcontratadas as seguintes parcelas do objeto:

4.17.1.1. Poderão ser subcontratadas parcelas do serviço, como, por exemplo, o monitoramento de primeiro nível pelo SOC/NOC

4.17.2. 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 o Contratante pelo rigoroso cumprimento das obrigações contratuais correspondentes ao objeto da subcontratação.

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

4.17.3.1. A contratada apresentará à Administração documentação que comprove a capacidade técnica da subcontratada, que será avaliada e juntada nos autos do processo correspondente.

4.18. É vedada a subcontratação completa ou da parcela principal da obrigação, abaixo discriminada:

4.18.1. O profissional sênior dedicado, considerado o núcleo da expertise e do relacionamento técnico com o STM.

4.19. É vedada a subcontratação de pessoa física ou jurídica, se aquela ou os dirigentes desta mantiverem 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 contratação ou atue na fiscalização ou na gestão do contrato, ou se deles forem cônjuge, companheiro ou parente em linha reta, colateral, ou por afinidade, até o terceiro grau.

Garantia da contratação

4.20. 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% (cinco por cento)** do **valor anual** da contratação.

4.21. A garantia nas modalidades caução, fiança bancária e título de capitalização deverá ser prestada em em até 1 (um) mês após assinatura do contrato.

4.22. No caso de seguro-garantia, regulamentado pela Circular SUSEP nº 662, de 2022, sua apresentação deverá ocorrer, no máximo, até a data de [assinatura do *contrato*.

4.22.1. A apólice deverá contemplar o pagamento de todos os eventos previstos contratualmente, além de ter validade durante a vigência do contrato e por mais 90 (noventa) dias após o término da vigência contratual, permanecendo em vigor mesmo que a contratada não pague o prêmio nas datas convencionadas.

4.22.2. Havendo fundamentado risco de prejuízo administrativo com a não assinatura do contrato, como, exemplificativamente, a interrupção de serviço contínuo, a Administração poderá, desde que obtida expressa anuência do licitante vencedor, bloquear o valor correspondente à garantia contratual do primeiro pagamento devido pela execução da contratação, ou dos pagamentos subsequentes, na hipótese de o primeiro se mostrar insuficiente.

4.22.3. O bloqueio de créditos previsto no subitem anterior implica constituição provisória de garantia, não gera direito a nenhum tipo de compensação financeira à contratada e deve ser liberado, tão logo a contratada apresente o seguro-garantia.

4.22.4. Na hipótese de ausência da expressa anuência referida no subitem 4.19.2., a não prestação de garantia, ultrapassado o prazo para entrega do seguro-garantia, configura comportamento faltoso, sujeito às sanções cabíveis.

4.22.5. Sem prejuízo do disposto no subitem 4.19.3., na hipótese de ausência da expressa anuência referida no subitem 4.19.2., será facultado à Administração, ultrapassado o prazo para entrega do seguro-garantia, perder interesse na celebração da contratação com o particular em mora.

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

Vistoria

4.24. Não há necessidade de realização de avaliação prévia do local de execução dos serviços.

5. MODELO DE EXECUÇÃO DO OBJETO

Condições de execução

5.1. A execução do objeto seguirá a seguinte dinâmica:

5.1.1. Início da execução do objeto: A implantação da solução deverá ser iniciada em até 30 (trinta) dias contados da emissão da primeira Ordem de Serviço. O planejamento e a execução deverão garantir que a nova solução esteja plenamente operacional a partir de janeiro de 2026, para assegurar a continuidade dos serviços de proteção de perímetro, visto que o contrato vigente se encerra em dezembro de 2025.

5.1.2. Descrição detalhada dos métodos, rotinas e procedimentos de execução: A prestação do serviço abrange todo o ciclo de vida da solução de segurança de perímetro, desde a implantação até a operação contínua e o suporte, conforme detalhado abaixo:

5.1.2.1. Implantação e Migração:

5.1.2.1.1. A CONTRATADA será responsável pela **instalação, configuração, integração e ativação** de todos os equipamentos NGFW com SD-WAN.

5.1.2.1.2. Deverá ser elaborado um **Plano de Migração** em conjunto com a equipe do STM, detalhando todas as etapas do processo, para minimizar impactos nas operações.

5.1.2.1.3. A migração efetiva do tráfego para a nova solução (*cutover*) será realizada em **janelas de manutenção programadas**, preferencialmente em fins de semana ou em horários de baixo expediente.

5.1.2.2. Operação Contínua do Serviço Gerenciado:

5.1.2.2.1. **Monitoramento e Gerenciamento (SOC/NOC):** A CONTRATADA deverá fornecer monitoramento proativo de segurança e desempenho, **24 horas por dia, 7 dias por semana**, através de seu Centro de Operações de Segurança/Rede (SOC/NOC).

5.1.2.2.2. **Gestão de Políticas:** A CONTRATADA será responsável por implementar e gerenciar continuamente as políticas de segurança definidas pelo STM, incluindo regras de firewall, IPS, Antivírus/Anti-malware, filtro de URL, controle de aplicações e SD-WAN.

5.1.2.2.3. Suporte Técnico Especializado: A CONTRATADA alocará **01 (um) profissional sênior de forma exclusiva e contínua** para o ambiente do STM. Este profissional atuará como ponto focal para suporte avançado (Nível 2 e 3), otimização de políticas (*tunning*), análise de desempenho, gestão de conectividade e resolução proativa de problemas complexos.

5.1.2.2.4. **Manutenção Integral:** O serviço inclui a manutenção preventiva, corretiva, adaptativa e evolutiva para todos os equipamentos e softwares da solução, sem ônus adicional para a Contratante .

5.1.3. Cronograma de realização dos serviços:

5.1.3.1. A implantação será realizada em fases, conforme a estratégia de uso da Ata de Registro de Preços (SRP) definida no ETP :

5.1.3.1.1. **Fase 1 – Implantação da Infraestrutura Crítica (Execução Imediata):**

5.1.3.1.1.1. **O que:** Instalação dos 2 (dois) equipamentos **Tipo I (Concentrador)** em alta disponibilidade no Data Center da Sede do STM e do **Serviço de Gerência Centralizada**.

5.1.3.1.1.2. **Quando:** Esta fase é prioritária e deverá ser iniciada logo após a emissão da primeira Ordem de Serviço.

5.1.3.1.2. **Fase 2 – Implantação nas Auditorias Remotas (Execução Sob Demanda):**

5.1.3.1.2.1. **O que:** Instalação dos equipamentos **Tipo II (1 unidade), Tipo III (3 unidades) e Tipo IV (12 unidades)** nas 16 Auditorias remotas.

5.1.3.1.2.1. **Quando:** A implantação ocorrerá de forma planejada e faseada ao longo da vigência da Ata de Registro de Preços (12 meses), mediante emissão de Ordens de Serviço específicas para cada localidade ou grupo de localidades, permitindo ao STM coordenar a logística de forma eficiente.

Local da prestação dos serviços

5.2. Os serviços, incluindo a instalação dos equipamentos e eventuais atendimentos presenciais, deverão ser prestados nos seguintes endereços da Justiça Militar da União:

Superior Tribunal Militar - Sede: Setor de Autarquias Sul Q. 1 - Asa Sul, Brasília - DF, 70098-900.

1ª Auditoria da 3ª CJM (Porto Alegre): Rua General Portinho 426 – Centro

2ª Auditoria da 3ª CJM (Bagé): Rua Monsenhor Costábile Hipólito 465

3ª Auditoria da 3ª CJM (Santa Maria): Alameda Montevideo, 244, Nossa Sra. das Dores

Arquivo do STM: SIA Trecho 17 - Parque Ferroviario De Brasilia, Brasília - DF, 71200-260.

Auditoria da 4ª CJM (Juiz de Fora) : Rua Mariano Procópio, nº 820-B

Auditoria da 5ª CJM (Curitiba): Rua Paulo Ildefonso de Assumpção, 92 – Bairro Bacacheri

Auditoria da 6ª CJM (Salvador): Av. Luiz Viana Filho (Paralela), 1600 – SMUS - Paralela

Auditoria da 7ª CJM (Recife): Avenida Engenheiro Domingos Ferreira, 3510, bairro de Boa Viagem

Auditoria da 8ª CJM (Belém): Av. Governador José Malcher, 611 - Nazaré

Auditoria da 9ª CJM (Campo Grande): Rua Terenos, 525 - Amambaí

Auditoria da 10ª CJM (Fortaleza): Av. Borges de Melo, 1711- Bairro Parreão

Auditoria da 12ª CJM (Manaus): Av. do Expedicionário, 2835 – São Jorge

ENAJUM: Setor de Garagens Oficiais Norte - SGON, Quadra 05, Lotes 05 e 06 - Brasília, DF, 70610-650.

Foro da 1ª CJM (Rio de Janeiro): Praia Belo Jardim, 555 – Ilha do Governador

Foro da 2ª CJM (São Paulo): Avenida Cásper Líbero, 88, 1º andar - Centro

Foro da 11ª CJM (Brasília): Setor de Autarquias Sul, Quadra 03, Lote 3A

5.3. Os serviços serão prestados nos seguintes horários, a depender da natureza da atividade:

5.3.1. **Monitoramento, Detecção e Resposta a Incidentes Críticos (P1) e Altos (P2):** O serviço de monitoramento proativo de segurança, realizado pelo Centro de Operações de Segurança (SOC/NOC) da contratada, bem como o atendimento e o início da solução para incidentes de prioridade Crítica e Alta, ocorrerá de forma ininterrupta, em regime de **24 horas por dia, 7 dias por semana (24x7x365)**.

5.3.2. **Suporte Presencial do Profissional Dedicado:** Quando solicitado pelo STM, as atividades presenciais do profissional sênior dedicado deverão ser realizadas nas dependências da Contratante em **horário comercial, das 12h às 19h, em dias úteis**, sem ônus adicionais.

5.3.3. **Atendimento a Incidentes de Média (P3) e Baixa (P4) Prioridade e Requisições de Serviço Padrão:** O atendimento e a solução para incidentes de menor criticidade, bem como a execução de requisições de serviço padrão (não emergenciais), ocorrerão em **Horário Comercial, de segunda a sexta-feira, das 09:00 às 19:00 (horário de Brasília-DF)**, conforme definido no Acordo de Nível de Serviço (SLA).

Rotinas a serem cumpridas:

5.4. A execução contratual observará as rotinas abaixo:

5.4.1. Emissão de Relatórios Mensais:

A CONTRATADA deverá fornecer ao STM, até o 5º dia útil de cada mês, um relatório detalhado contendo o desempenho do serviço no mês anterior. O relatório deve incluir, no mínimo:

a) Lista de todos os incidentes e requisições de serviço, com seus respectivos horários de abertura, resposta e solução;

b) Cálculo do cumprimento de todas as métricas de SLA;

c) Cálculo da disponibilidade mensal do serviço;

d) Análise de causa raiz para todos os incidentes de prioridade P1 e P2;

e) Sumário executivo das atividades realizadas pelo profissional dedicado.

5.4.2. Entrega de Backups de Configuração:

A CONTRATADA será obrigada a fornecer ao STM, **trimestralmente** ou sempre que houver alteração relevante, um backup completo e atualizado de todas as configurações da solução. Este backup é um ativo estratégico do STM para garantir a continuidade e a independência tecnológica.

5.4.3. **Elaboração e Manutenção de Documentação Técnica:** A CONTRATADA será responsável por elaborar e manter atualizada toda a documentação técnica da solução, incluindo, mas не se limitando a:

a) Plano de Implantação e Migração, a ser elaborado em conjunto com o STM no início do contrato;

b) Diagramas de rede e topologia da solução;

c) Manuais de procedimentos específicos do ambiente do STM.

5.4.4. Capacitação da Equipe Técnica do STM:

A CONTRATADA deverá fornecer um treinamento, oficial ou customizado, para no mínimo **5 (cinco) técnicos** da equipe da DITIN. O treinamento deverá abranger a arquitetura da solução, o uso da console de gerenciamento (modo visualização), a geração de relatórios e os procedimentos de abertura de chamados, visando capacitar a equipe do STM para uma fiscalização eficaz do contrato.

5.4.5. **Reuniões de Acompanhamento:** O profissional sênior dedicado deverá estar disponível para participar de reuniões periódicas (virtuais ou presenciais) com a equipe do STM para discutir o desempenho do serviço, analisar relatórios, planejar melhorias e alinhar as estratégias de segurança da informação.

Materiais a serem disponibilizados

5.5. Para a perfeita execução dos serviços, a contratada deverá disponibilizar todos os materiais, equipamentos, softwares, licenças e recursos humanos necessários, nas quantidades e qualidades estabelecidas, promovendo sua substituição quando necessário, sem ônus adicional ao Contratante. A disponibilização inclui, no mínimo:

5.5.1. Equipamentos de Hardware (NGFW com SD-WAN):

Todos os equipamentos deverão ser novos, sem uso anterior, em linha de produção e em sua versão mais atualizada. A CONTRATADA deverá fornecer:

a) 02 (dois) equipamentos **Tipo I (Concentrador)**;

b) 01 (um) equipamento **Tipo II (Unidade Remota de Grande Porte)**;

c) 03 (três) equipamentos **Tipo III (Unidades Remotas de Médio Porte)**;

d) 12 (doze) equipamentos **Tipo IV (Unidades Remotas de Pequeno Porte)**.

5.5.2. Software e Licenciamento:

Fornecimento de todas as licenças de software (subscrições) necessárias para a plena operação de todas as funcionalidades de segurança e gerenciamento da solução, durante os 60 (sessenta) meses de vigência do contrato. As licenças deverão ser emitidas em nome da **Contratante (STM)**.

5.5.3. Plataforma de Gerenciamento Centralizado:

Disponibilização da solução para gerenciamento unificado, centralização de logs, eventos e relatórios de todos os 18 (dezoito) equipamentos de proteção de perímetro.

5.5.4. **Recursos Humanos Especializados:**

a) **Profissional Sênior Dedicado:** Alocação de, no mínimo, 01 (um) profissional sênior, de forma exclusiva e contínua, para gerenciamento, administração e suporte avançado de todos os serviços e equipamentos.

b) **Equipe de Suporte (SOC/NOC):** Disponibilização de equipe técnica em seu Centro de Operações de Segurança/Rede (SOC/NOC) para monitoramento proativo e atendimento a incidentes em regime 24x7.

5.5.5. **Ferramentas e Acessórios:** Todos os demais materiais, ferramentas, utensílios e acessórios (cabos, conectores, etc.) necessários para a correta instalação, configuração, manutenção e substituição dos equipamentos são de responsabilidade da CONTRATADA.

Informações relevantes para o dimensionamento da proposta

5.6. A demanda do órgão tem como base as seguintes características, que devem ser consideradas pelos licitantes na elaboração de suas propostas:

5.6.1. Abrangência Geográfica e Diversidade de Ambientes:

A solução deverá ser implantada em **17 (dezessete) localidades distintas** da Justiça Militar da União, distribuídas pelo território nacional. Essas localidades possuem portes e demandas de tráfego diferentes, o que justifica a especificação de quatro tipos de equipamentos (I, II, III e IV) com perfis de desempenho distintos.

5.6.2. Requisito de Alta Disponibilidade na Sede:

Os dois equipamentos do Tipo I, destinados ao Data Center da Sede do STM, deverão ser configurados e implantados para operar em um **cluster de Alta Disponibilidade (Ativo/Passivo)**, garantindo a redundância e a continuidade dos serviços em caso de falha de um dos equipamentos.

5.6.3. **Integração com a Infraestrutura Existente:** A solução não será implantada em um ambiente isolado, devendo obrigatoriamente se integrar com a infraestrutura de TIC já existente no STM. As principais interdependências são: **Links de Comunicação:** A funcionalidade SD-WAN irá gerenciar os links de internet e de comunicação de dados já contratados pelo STM.

Especificação da garantia do serviço

5.7. A garantia da solução completa (incluindo todos os equipamentos de hardware, softwares e seus componentes) e a prestação dos serviços de suporte e manutenção deverão ser integrais e válidas durante todo o prazo de vigência do contrato, ou seja, por **60 (sessenta) meses**.

5.7.1. Isto implica que a CONTRATADA é responsável por reparar ou substituir, sem qualquer ônus para o Contratante, qualquer componente que apresente falha ou defeito durante a vigência contratual, assegurando a contínua operacionalidade da solução e o cumprimento dos prazos definidos no Acordo de Nível de Serviço (SLA).

5.7.2. A exigência de uma garantia integral e coextensiva ao prazo do contrato é um requisito indissociável do modelo de contratação escolhido. A justificativa se baseia em dois pilares fundamentais:

5.7.2.1. **Natureza da Contratação (Serviço vs. Aquisição):** O objeto da contratação é a prestação de um "Serviço Gerenciado de Segurança", e não a simples aquisição de equipamentos . Os ativos de hardware e software são ferramentas para a entrega do serviço, permanecendo como propriedade da contratada . Desta forma, a obrigação da contratada não é apenas entregar os equipamentos, mas garantir sua plena e contínua operacionalidade durante todo o período contratual. A garantia integral, portanto, não é um adicional, mas a própria essência do serviço de assegurar a "continuidade e estabilidade", minimizando interrupções.

5.7.2.2. **Alinhamento com a Vigência Contratual:** Uma vez que a prestação de serviços e o contrato como um todo terão vigência de 60 meses, a garantia de todos os seus componentes (equipamentos e softwares) deve, obrigatoriamente, possuir a mesma duração . Um prazo de garantia inferior ao da vigência do contrato seria ineficaz, pois deixaria o STM com uma solução desprotegida e sem suporte do fabricante em caso de falhas a partir do término da garantia, inviabilizando a própria continuidade do serviço pago mensalmente.

5.8. Os serviços de manutenção e assistência técnica, quando necessitarem de atuação presencial, deverão ser realizados nas dependências da Contratante, em qualquer um dos endereços listados no item 5.2 deste Termo de Referência.

5.8.1. O técnico da CONTRATADA deverá se deslocar ao local da repartição que demandar o atendimento, sempre que solicitado pelo STM. Este deslocamento e a prestação de serviço presencial não deverão gerar quaisquer ônus adicionais à Contratante, devendo todos os custos estarem inclusos no valor mensal do serviço.

Procedimentos de transição e finalização do contrato

5.9. Serão necessários procedimentos de transição contratual. A CONTRATADA deverá obrigatoriamente observar as seguintes atividades no período de transição, que corresponderá aos **últimos 60 (sessenta) dias** de vigência do contrato:

5.9.1. Entrega de Ativos Lógicos e Documentação:

A CONTRATADA deverá entregar ao STM uma cópia final, completa e atualizada de todos os ativos lógicos e documentais do serviço. Isso inclui, no mínimo:

a) **Backups de Configuração:** Cópia completa das configurações de todos os equipamentos (NGFW e Gerência Centralizada), incluindo políticas de firewall, regras de NAT, configurações de VPN, objetos de rede, políticas de IPS e SD-WAN.

b) **Documentação Técnica:** Versão final de toda a documentação do ambiente, como diagramas de rede, topologia da solução e manuais de procedimentos.

5.9.2. Transferência Final de Conhecimentos:

A CONTRATADA deverá colaborar integralmente com a nova equipe que assumirá o serviço (seja de um novo fornecedor ou do próprio STM). Essa colaboração deverá incluir a realização de reuniões técnicas para explicar a arquitetura da solução e a lógica das políticas implementadas, com o profissional sênior dedicado disponível para sanar dúvidas e garantir uma transição suave.

5.9.3. Desinstalação e Remoção dos Equipamentos:

Sendo um contrato de serviço, a CONTRATADA será a única responsável pela logística de desinstalação e remoção de todos os seus equipamentos físicos das 17 localidades da JMU ao término do contrato. O processo deverá ser agendado em coordenação com a equipe da COTEC.

5.9.4. Revogação de Perfis de Acesso:

No último dia de vigência do contrato, todos os perfis de acesso, lógicos e físicos, concedidos à equipe da CONTRATADA (administradores, VPN, crachás, etc.) deverão ser formalmente revogados e o procedimento auditado pela equipe de segurança do STM.

Comprovação de Qualificação da Equipe Técnica Mínima, especificamente do **Profissional Sênior Dedicado** que será alocado ao contrato, por meio de:

5.10. Experiência Profissional: Comprovação de que o profissional possui experiência mínima de **3 (três) anos**, na atuação direta com soluções de NGFW, incluindo atividades de implantação, configuração e suporte técnico. A comprovação poderá ser feita mediante apresentação de currículo detalhado acompanhado de declarações de empresas, contratos de trabalho ou outros documentos idôneos.

5.11. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.

5.12. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do licitante.

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

5.14. Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

6. MODELO DE GESTÃO DO CONTRATO

6.1. 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.

6.2. 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.

6.3. As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade.

6.3.1. As comunicações formais entre o órgão e a contratada devem ser feitas na forma de intimação administrativa eletrônica do Sistema Eletrônico de Informações (SEI), conforme Ato Normativo 430, de 2020, reservado o uso de correio eletrônico institucional, via SEI, ou o uso de aplicativo de mensagem para telefone móvel como complemento dessa notificação.

6.3.2. As comunicações entre o órgão e a contratada poderão ser feitas diretamente por meio de correio eletrônico institucional, via SEI, ou por meio de aplicativo de mensagem para telefone móvel, quando a situação exija celeridade ou quando a comunicação aborde atividades corriqueiras relativas à execução contratual, hipóteses em que deverá ser juntado aos autos o registro do diálogo ou a certidão da fiscalização, atestando a sua ocorrência.

6.3.3. O Manual para Usuários Externos do SEI-JMU encontra-se disponível em https://www.stm.jus.br/sei-stm/orientacoes.

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

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

6.5.1. Os assuntos tratados na reunião inicial serão registrados em ata ou documento equivalente, com vistas a comprovar sua realização.

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

6.6.1. A contratada não necessitará manter preposto da empresa no local da execução do objeto durante o período contratual.

6.6.1.1. A CONTRATADA deverá indicar formalmente, no prazo de 5 (cinco) dias úteis após a assinatura do contrato, os dados de contato (nome, cargo, e-mail e telefone) de seu preposto e do profissional sênior dedicado, bem como o procedimento para seu acionamento.

6.6.2. A Contratante poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que a contratada designará outro para o exercício da atividade.

6.7. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput).

6.8. O fiscal técnico 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;

6.8.1. O fiscal técnico anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas a sua execução, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei nº 14.133, de 2021, art. 117, §1º);

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

6.8.3. O fiscal técnico do contrato informará ao gestor, 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;

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

6.8.5. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou à prorrogação contratual;

6.8.6. O fiscal técnico 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;

6.8.6.1. Caso ocorram descumprimento das obrigações contratuais, o fiscal técnico do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência.

6.9. Além do disposto acima, a fiscalização técnica do contrato obedecerá às seguintes rotinas:

6.9.1. Analisar e validar tecnicamente os relatórios mensais de desempenho e de cumprimento do Acordo de Nível de Serviço (SLA) apresentados pela CONTRATADA.

6.9.2. Atuar como ponto focal técnico do STM para a abertura, acompanhamento e validação da resolução de incidentes de segurança e problemas técnicos.

6.9.3. Avaliar e aprovar tecnicamente as solicitações de mudança nas configurações e políticas de segurança, como a criação ou alteração de regras de firewall.

6.9.4. Comunicar ao Gestor do Contrato, em tempo hábil, qualquer situação que demande decisão ou medida que ultrapasse sua competência.

6.10. O gestor do contrato coordenará as atividades relacionadas à execução e à fiscalização, bem como dos atos preparatórios à instrução processual e ao encaminhamento da documentação pertinente para a formalização dos procedimentos relativos à prorrogação, à alteração, ao reequilíbrio, ao pagamento, à eventual aplicação de sanções e à extinção dos contratos.

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

6.10.2. O gestor do contrato, quanto este ato não for atribuído para comissão, emitirá, por meio do Termo de Recebimento Definitivo, documento comprobatório da avaliação realizada pelos fiscais técnico e, se for o caso, setorial quanto ao cumprimento de obrigações assumidas pela contratada, com menção ao seu desempenho na execução contratual, baseado, se houver, nos indicadores objetivamente definidos e aferidos.

6.10.2.1. O gestor do contrato, caso a execução ocorra por etapas, também promoverá a homologação dos atestes das etapas e encaminhará para pagamento.

6.10.4. O gestor do contrato apresentará, no Relatório de Irregularidades Contratuais, parecer fundamentado sobre a existência (ou não) de elementos informativos suficientes para 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.

6.10.5. O gestor do contrato deverá, com o apoio dos registros dos fiscais, manter atualizado o mapa de riscos elaborado na fase de planejamento da contratação, após a ocorrência de eventos relevantes.

6.11. 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.

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

6.13. A fiscalização administrativa não exclui nem reduz a responsabilidade da contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vício redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade da Contratante ou de seus agentes, gestores e fiscais, de conformidade.

7. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

7.1. A avaliação da execução do objeto e a medição dos resultados para fins de pagamento serão realizadas com base no **Acordo de Nível de Serviço (SLA)**, cujas métricas, metas e penalidades estão detalhadas no Anexo I - REQUISITOS TÉCNICOS E SLA deste Termo de Referência, em conformidade com o planejado no ETP.

7.2. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, conforme os percentuais e as condições estabelecidas no SLA, sem prejuízo de outras sanções cabíveis.

7.3. A aferição considerará, no mínimo, os seguintes critérios definidos no SLA:

a) Cumprimento dos **Tempos de Resposta e de Solução** para incidentes (Prioridades P1, P2, P3 e P4).

b) Atingimento da meta de **Disponibilidade Mínima Mensal** de 99,9% para os serviços críticos.

c) Cumprimento dos prazos para **Requisições de Serviço**.

Do recebimento

7.4. Os serviços serão recebidos provisoriamente, no prazo de 10 (dez) dias, pelo fiscal técnico, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo. (Art. 140, I, a , da Lei nº 14.133, de 2021)

7.4.1. O prazo da disposição acima será contado do recebimento da nota fiscal.

7.4.2. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante Termo de Recebimento Provisório - Serviços Comuns que comprove o cumprimento das exigências de caráter técnico.

7.4.3. O fiscal setorial do contrato, quando houver, realizará o ateste setorial, sob o ponto de vista técnico e administrativo funcional, objetivando verificar o atendimento dos fins a que se propôs a contratação.

7.5. 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 a análise do desempenho e qualidade da prestação dos serviços realizados, se houver, 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.

7.5.1. A contratada fica obrigada 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.

7.5.2. 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. (Art. 119 c/c art. 140 da Lei nº 14133, de 2021).

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

7.5.4. 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.

7.6. Quando a fiscalização for exercida por um único servidor, o Termo de Recebimento Provisório - Serviços Comuns 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.

7.7. Os serviços serão recebidos definitivamente pelo gestor ou por comissão designada pela autoridade competente, no prazo de 3 (três) dias úteis, contados do envio do processo pelo fiscal técnico, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

7.7.1. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico e setorial, quando houver, no cumprimento de obrigações assumidas pela contratada, com menção ao seu desempenho na execução contratual, baseado, se houver, em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas.

7.7.2. 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;

7.7.3. Emitir termo circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas;

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

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

7.9. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pela contratada, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

7.10. 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.

Liquidação

7.11. Recebida a Nota Fiscal ou documento de cobrança equivalente, o setor competente, para fins de liquidação, deverá verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

7.11.1. o prazo de validade;

7.11.2. a data da emissão;

7.11.3. os dados do contrato e do órgão contratante;

7.11.4. o período respectivo de execução do contrato;

7.11.5. o valor a pagar;

7.11.6. eventual destaque do valor de retenções tributárias cabíveis; e

7.11.7. descrição do valor unitário e quantidade dos itens do serviço prestado.

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

7.13. 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, de 2021.

7.14. A Administração deverá realizar consulta ao SICAF para:

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

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

7.15. Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 60 (sessenta) dias corridos, contado da confirmação de recebimento do ofício, regularize sua situação ou, no mesmo prazo, apresente sua defesa.

7.16. Persistindo a irregularidade, o Contratante deverá instaurar procedimento de rescisão contratual, assegurada à contratada a ampla defesa.

7.16.1. Na notificação para exercício da ampla defesa, a contratada será informada de que, em caso de regularização no prazo de 30 (trinta) dias corridos, contado da confirmação do recebimento do ofício, o procedimento será interrompido, com a manutenção automática da contratação. A contratada também será informada de que, passado o referido prazo sem a regularização, o procedimento de rescisão terá continuidade, com decisão da autoridade competente acerca do encerramento prematuro da contratação, a partir dos elementos de fato e de direito colhidos na instrução do feito.

7.16.2. A decisão da autoridade competente, ao final do procedimento de rescisão, de manutenção da contratação, a despeito da permanência da irregularidade, deverá ser acompanhada de justificativa de que a continuidade da contratação é a medida mais vantajosa para a Administração, podendo o Gestor, para melhor avaliação da situação, ser convocado para mapear os riscos envolvidos com o encerramento prematuro.

7.17. Durante a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, comunicando à Fazenda Pública e demais Órgãos responsáveis, conforme o caso.

Prazo de pagamento

7.18. O pagamento será efetuado no prazo de 30 (trinta) dias contados da conclusão do Termo de Ateste - Serviços Comuns, conforme seção anterior.

7.19. Nos casos de eventuais atrasos de pagamento, desde que a contratada não tenha concorrido de alguma forma para o fato, a atualização financeira devida, entre a data que deveria ser efetuado o pagamento e a data correspondente ao efetivo pagamento, será calculada da seguinte forma, devendo a atualização prevista nesta condição ser incluída em nota fiscal a ser apresentada posteriormente:

AF = I x N x VP

AF = atualização financeira devida;

I = 0,0001644 (índice de atualização dia);

N = número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = valor do pagamento devido.

Forma de pagamento

7.20. O pagamento será realizado através de ordem bancária, para crédito em banco, agência e conta corrente indicados pela contratada.

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

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

7.22.1. 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.

7.23. A contratada 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.

8. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

Critério de Julgamento

8.1. O julgamento da proposta ocorrerá pelo critério de menor preço.

Regime de Execução

8.2. O regime de execução do contrato será fornecimento e prestação de serviço associado.

Exigências de qualificação técnica

8.3. Para fins de qualificação técnica, deverá o licitante comprovar os seguintes requisitos:

8.4. **Comprovação de aptidão para execução de serviço de complexidade tecnológica e operacional equivalente ou superior**, por meio da apresentação de um ou mais Atestado(s) de Capacidade Técnica, fornecido(s) por pessoa jurídica de direito público ou privado, que comprove(m) que o licitante executou ou executa contrato de **serviços gerenciados de segurança de perímetro (NGFW) com monitoramento proativo (SOC/NOC)**.

8.4.1. O(s) atestado(s) deverá(ão) comprovar a prestação dos serviços por um período mínimo de **12 (doze) meses contínuos**.

8.4.2. O(s) atestado(s) deverá(ão) comprovar a gestão de um ambiente com, no mínimo, **5 (cinco) dispositivos** de segurança de perímetro.

Justificativa: A exigência de comprovação de aptidão técnica, por meio de Atestado(s) de Capacidade Técnica que demonstrem experiência prévia em "serviços gerenciados de segurança de perímetro (NGFW) com monitoramento proativo (SOC/NOC)", é uma medida indispensável para garantir o cumprimento das obrigações contratuais e a segurança da infraestrutura crítica da Justiça Militar da União (JMU), fundamentando-se nos seguintes pontos:

Natureza Crítica e Complexa do Objeto: A contratação não se resume à aquisição de equipamentos, mas à prestação de um **Serviço Gerenciado de Segurança da Informação**. Este serviço é um pilar para a proteção dos ativos de informação e para a garantia da continuidade dos serviços jurisdicionais da JMU , que enfrenta ameaças cibernéticas cada vez mais sofisticadas. Uma falha na execução deste contrato pode resultar na paralisação de sistemas essenciais, como o e-Proc/JMU, causando prejuízos incalculáveis e interrupção da prestação jurisdicional. Portanto, é imperativo que a contratada possua experiência comprovada na gestão de ambientes de alta criticidade.

O Foco é o Serviço Gerenciado: O Estudo Técnico Preliminar (ETP) diagnosticou como uma fraqueza institucional a "Equipe insuficiente para o quantitativo de demandas de TIC". A solução escolhida visa suprir essa carência, transferindo a responsabilidade da operação, monitoramento 24x7 e resposta a incidentes para uma empresa especializada, que possua um Centro de Operações de Segurança/Rede (SOC/NOC). Exigir a comprovação de experiência específica em serviços gerenciados com monitoramento proativo é a única forma de garantir que a licitante possui a capacidade operacional e a maturidade de processos necessárias para entregar o principal valor agregado do contrato: a gestão especializada e contínua da segurança.

Mitigação de Riscos Técnicos e Operacionais: A administração de uma solução de NGFW em um ambiente corporativo crítico envolve a configuração complexa de regras, tratamento de incidentes, análise de novas versões de software e otimização contínua. Atestar a experiência prévia da licitante nessas atividades mitiga o risco de contratar uma empresa sem o conhecimento prático necessário, o que poderia expor a JMU a falhas de segurança, indisponibilidade de serviços e descumprimento de normativos, como a Resolução CNJ nº 396/2021.

Conclui-se que a exigência de qualificação técnica é estritamente pertinente e proporcional à complexidade e à criticidade do objeto a ser contratado, sendo uma salvaguarda essencial para o interesse público e para a segurança das operações do Poder Judiciário.

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

8.7. A apresentação, pelo licitante, de certidões ou atestados de desempenho anterior emitido em favor de consórcio do qual tenha feito parte será admitida, desde que atendidos os requisitos do art. 67, §§ 10 e 11, da Lei nº 14.133, de 2021, e regulamentos sobre o tema.

8.8. A licitante deverá apresentar declaração de que o profissional sênior indicado para dedicação exclusiva não possui outros compromissos que inviabilizem o cumprimento desta obrigação durante a vigência do contrato.

Da Apresentação da Proposta Técnica

8.9. A Proposta Técnica deverá conter o detalhamento de todos os equipamentos, softwares e serviços ofertados, demonstrando o cumprimento integral de todas as especificações contidas neste Termo de Referência e em seus anexos.

8.10. Adicionalmente, a LICITANTE deverá fornecer, como parte integrante de sua Proposta Técnica, uma **planilha de conformidade (ponto-a-ponto)**, em formato editável (ex: .xlsx, .ods), indicando, para cada um dos requisitos das especificações técnicas (ANEXO I, deste Termo de Referência), o documento e a respectiva página de sua proposta onde consta a comprovação de seu cumprimento.

8.10.1. Salvo onde está especificado explicitamente no requisito, não serão aceitas referências a futuros releases ou versões de produtos para comprovar a existência ou aderência a qualquer quesito desta especificação;
8.10.2. Cada documento apresentado deve descrever claramente a referência ao modelo apresentado na proposta, não sendo válidas referências genéricas;
8.10.3. Será aceita Carta do Fabricante, como comprovação de atendimento de requisitos técnicos e de compatibilidade especificados neste edital, apenas para os itens que não constarem na documentação da maioria dos fabricantes ou que não puderem ser mensurados.

8.10.4. A planilha deverá apresentar o seguinte formato:

Item / Requisito Técnico do Edital	Descrição do Requisito (copiar do TR/edital)	Atendimento pelo Licitante (Sim/Não)	Comprovação / Evidência	Página / Documento de Referência	Observações

8.10.5. A planilha de composição de preços/proposta detalhada servirá como documento de suporte para a análise da proposta, sendo sua apresentação obrigatória. O preenchimento incorreto ou incompleto, desde que se trate de falhas formais que não comprometam a essência da proposta (tais como erros de soma, omissão de informações não essenciais, etc.), será objeto de diligência para saneamento por parte do agente de contratação ou da comissão, nos termos do art. 64, § 1º, da Lei nº 14.133/2021. A desclassificação ocorrerá apenas se as falhas ou a não apresentação da planilha configurarem vício insanável que impeça a aferição do cumprimento dos requisitos técnicos ou a análise da exequibilidade dos preços, conforme o art. 59, V, da mesma Lei.

9. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

9.1. O custo estimado da contratação possui caráter sigiloso e será tornado público apenas e imediatamente após o julgamento das propostas.

9.1.1. O caráter sigiloso do orçamento estimado para a contratação não prevalecerá para os órgãos de controle interno e externo.

9.1.2. Justificativa para Adoção do Orçamento Sigiloso (Subitem 9.1)

9.1.2.1. A decisão administrativa de adotar o caráter sigiloso para o orçamento estimado desta contratação fundamenta-se no Art. 24 da Lei nº 14.133, de 2021 , e tem como objetivo principal **ampliar a competitividade do certame e, consequentemente, assegurar a seleção da proposta mais vantajosa para a Administração Pública**.

9.1.2.2. A estratégia se justifica pelos seguintes motivos:

9.1.2.2.1. **Estímulo à Formulação de Propostas Genuínas:** Ao não divulgar o valor de referência, os licitantes são incentivados a formular suas propostas com base em suas próprias estruturas de custos, eficiências operacionais e condições de mercado, em vez de simplesmente ancorar seus preços em um valor máximo estipulado pela Administração. Isso fomenta uma competição mais autêntica e pode resultar na obtenção de preços significativamente inferiores aos estimados.

9.1.2.2.2. **Mitigação do Risco de Preços "Acomodados":** A publicidade do orçamento estimado pode, em certos mercados, levar a um alinhamento estratégico de propostas em um patamar ligeiramente inferior ao valor máximo admitido, sem que este represente, de fato, o menor preço que o mercado poderia oferecer. O sigilo do orçamento mitiga esse risco, tornando o ambiente de disputa mais propenso à busca pela real vantajosidade econômica.

9.1.2.2.3. **Contexto de Mercado Competitivo:** Conforme apurado no Estudo Técnico Preliminar (ETP), o mercado de soluções de segurança de perímetro (NGFW) e Serviços Gerenciados de Segurança (MSS) é maduro e altamente competitivo, com múltiplos fornecedores de tecnologia e empresas integradoras aptas a participar do certame. O orçamento sigiloso é a ferramenta estratégica mais eficaz para potencializar essa competitividade em benefício do interesse público.

9.1.2.2.4. **Preservação da Transparência:** A medida não fere o princípio da transparência, uma vez que o sigilo é temporário. O valor estimado será tornado público imediatamente após a fase de julgamento das propostas, permitindo o pleno controle social e dos órgãos de fiscalização sobre a economicidade da contratação. Todos os demais elementos necessários à elaboração das propostas, como o detalhamento dos quantitativos e as especificações técnicas, são públicos e constam neste Termo de Referência.

9.2. Em caso de licitação para Registro de Preços, 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 oras ou dos serviços registrados, nas seguintes situações:

9.2.1. em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizam a execução da ata tal como pactuada, nos termos do disposto na alínea "d" do inciso II do caput do art. 124 da Lei nº 14.133, de 2021;

9.2.2. em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou superveniência de disposições legais, com comprovada repercussão sobre os preços registrados;

9.2.3. serão reajustados os preços registrados, respeitada a contagem da anualidade e o índice previsto para a contratação; ou

9.2.4. poderão ser repactuados, a pedido do interessado, conforme critérios definidos para a contratação.

10. OBRIGAÇÕES DO CONTRATANTE

10.1. Exigir o cumprimento de todas as obrigações assumidas pela contratada, de acordo com o contrato e seus anexos;

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

10.3. Notificar a contratada, por escrito, sobre vícios, defeitos, incorreções imperfeições, falhas ou irregularidades verificadas na execução do objeto contratual, fixando prazo para que seja substituído, reparado ou corrigido, total ou parcialmente, às suas expensas, certificando-se de que as soluções por ele propostas sejam as mais adequadas;

10.4. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pela contratada;

10.5. Comunicar a contratada para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133, de 2021;

10.6. Efetuar o pagamento à contratada do valor correspondente à execução do objeto, no prazo, forma e condições estabelecidos no presente Termo de Referência;

10.7. Aplicar à contratada as sanções previstas na lei e neste Termo de Referência;

10.8. Cientificar o órgão de representação judicial da Advocacia-Geral da União para adoção das medidas cabíveis quando do descumprimento de obrigações pela contratada;

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

10.9.1. A Administração terá o prazo de 1 (um) mês, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.

10.9.2. O prazo referido no subitem anterior ficará suspenso enquanto a contratada não cumprir os atos ou apresentar documentação requisitada pelo Contratante para análise da solicitação ou da reclamação.

10.10. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pela contratada no prazo máximo de 90 (noventa) dias.

10.10.1. O prazo referido no subitem anterior ficará suspenso enquanto a contratada não cumprir os atos ou apresentar documentação requisitada pelo Contratante para análise do pedido de reestabelecimento do equilíbrio econômico-financeiro.

10.11. Verificar, se for o caso, que a apólice de seguro foi registrada na Superintendência de Seguros Privados (SUSEP), devendo essa condição ser verificada, no sítio eletrônico https://www2.susep.gov.br/safe/apolices/app/garantia, após 7 (sete) dias úteis da sua emissão;

10.12. Notificar, se houver, os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

10.13 Comunicar a contratada na hipótese de posterior alteração do projeto pelo Contratante, no caso do art. 93, §2º, da Lei nº 14.133, de 2021.

10.14. A Administração não responderá por quaisquer compromissos assumidos pela contratada com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da contratada, de seus empregados, prepostos ou subordinados.

10.15. Fornecer atestado de capacidade técnica se solicitado pela contratada, desde que cumpridas todas as exigências contratuais;

10.16. Fornecer por escrito as informações necessárias para o desenvolvimento dos serviços pelo objeto da contratação;

10.17. Realizar avaliações periódicas da qualidade dos serviços, após seu recebimento;

10.18. Assegurar que o ambiente de trabalho, inclusive seus equipamentos e instalações, apresentem condições adequadas ao cumprimento, pela contratada, das normas de segurança e saúde no trabalho, quando o serviço for executado em suas dependências, ou em local por ela designado;

10.19. Previamente à expedição da ordem de serviço, verificar pendências, liberar áreas e/ou adotar providências cabíveis para a regularidade do início da sua execução;

10.20. É vedado ao Contratante manter 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, inclusive.

10.21 É vedada ao Contratante a contratação de 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, conforme art. 2º, inciso VI, da Resolução CNJ nº 07, de 2005, seguindo o definido no Ato Normativo STM nº 640, de 2023 (3205183);

10.21.1. A vedação constante deste subitem se estende às contratações cujo procedimento licitatório tenha sido deflagrado quando os magistrados e servidores geradores de incompatibilidade estavam no exercício dos respectivos cargos e funções, assim como às licitações iniciadas até 6 (seis) meses após a desincompatibilização.

10.21.2. A contratação de empresa pertencente a parente de magistrado ou servidor não abrangido pelas hipóteses expressas de nepotismo poderá ser vedada, quando, no caso concreto, for identificado risco potencial de contaminação do processo licitatório, conforme art. 2º, § 4º, da Resolução CNJ nº 07, de 2005.

10.22. É vedada a manutenção, aditamento ou prorrogação de contrato de prestação de serviços com empresa que venha a contratar empregados que sejam cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de ocupantes de cargos de direção e de assessoramento, de ministros ou juízes da respectiva Auditoria contratante, conforme art. 3º da Resolução CNJ nº 07, de 2005, seguindo o definido no Ato Normativo STM nº 640, de 2023 (3205183).

11. OBRIGAÇÕES DA CONTRATADA

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

11.2. Manter preposto aceito pela Administração, conforme padrão de gestão do contrato deste Termo de Referência.

11.2.1. A indicação ou a manutenção do preposto da empresa poderá ser recusada pelo órgão ou entidade, desde que devidamente justificada, devendo a empresa designar outro para o exercício da atividade.

11.3. Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior (art. 137, II) e prestar todo esclarecimento ou informação por eles solicitado;

11.4. Alocar os empregados necessários ao perfeito cumprimento do objeto, com habilitação e conhecimento adequados, 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;

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

11.6. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078, de 1990), 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;

11.7. Efetuar comunicação ao Contratante, assim que tiver ciência da impossibilidade de realização ou finalização do serviço no prazo estabelecido, para adoção de ações de contingência cabíveis;

11.8. Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, a contratada deverá entregar ao setor responsável pela fiscalização do contrato, junto com a Nota Fiscal para fins de pagamento, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda Estadual/Distrital e/ou Municipal/Distrital do domicílio ou sede da contratada, conforme exigido no Edital; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT;

11.9. 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;

11.10. Comunicar ao Fiscal do contrato tempestivamente, observada a urgência da situação, qualquer ocorrência anormal ou acidente que se verifique no local da execução do objeto contratual, não ultrapassando o prazo de 24 (vinte e quatro) horas;

11.11. 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 objeto contratado.

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

11.13. Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência contratual;

11.14. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina;

11.15. 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.

11.16. Cumprir as normas de proteção ao trabalho, inclusive aquelas relativas à segurança e à saúde no trabalho;

11.17. Não submeter os trabalhadores a condições degradantes de trabalho, jornadas exaustivas, servidão por dívida ou trabalhos forçados;

11.16. 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;

11.17. Não submeter o menor de dezoito anos de idade à realização de trabalho noturno e em condições perigosas e insalubres e à realização de atividades constantes na Lista de Piores Formas de Trabalho Infantil, aprovada pelo Decreto nº 6.481, de 2008;

11.18. Receber e dar o tratamento adequado a denúncias de discriminação, violência e assédio no ambiente de trabalho;

11.17. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação, ou para a qualificação na contratação direta;

11.18. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação (art. 116);

11.19. Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas (art. 116, parágrafo único);

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

11.21. 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;

11.22. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do Contratante;

11.23. Manter os empregados nos horários predeterminados pelo Contratante;

11.24. Apresentar os empregados devidamente identificados por meio de crachá;

11.25. Apresentar ao Contratante, quando for o caso, a relação nominal dos empregados que adentrarão no órgão para a execução do serviço;

11.26. Instruir seus empregados quanto à necessidade de acatar as Normas Internas do Contratante;

11.27. Insruir os seus empregados, quanto à prevenção de incêndios nas áreas do Contratante;

11.28. Adotar as providências e precauções necessárias, inclusiva a consulta nos respectivos órgãos, se necessário for, a fim de que não venham a ser danificadas as redes hidrossanitárias, elétricas e de comunicação;

11.29. A propriedade intelectual do software embarcado nos equipamentos e do sistema operacional do firewall pertence exclusivamente ao fabricante. O direito de uso pelo STM é garantido por meio das licenças (subscrições) fornecidas pela CONTRATADA.

11.29.1. No entanto, todo produto de trabalho intelectual desenvolvido especificamente para o STM no decorrer do contrato — como scripts de automação, modelos de relatórios customizados ou documentação técnica específica do ambiente — terá seus direitos de uso e modificação perpetuamente cedidos ao STM, sem custos adicionais, garantindo que o conhecimento customizado para a JMU seja retido pela instituição.

12. INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

12.1. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, a contratada que:

12.1.1. der causa à inexecução parcial do contrato;

12.1.2. der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

12.1.3. der causa à inexecução total do contrato;

12.1.4. ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

12.1.5. apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

12.1.6. praticar ato fraudulento na execução do contrato;

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

12.1.8. praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

12.2. Serão aplicadas à contratada que incorrer nas infrações acima descritas as seguintes sanções:

12.2.1. **Advertência**, quando a contratada 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);

12.2.2. **Impedimento de licitar e contratar**, quando praticadas as condutas descritas nas alíneas 12.1.2., 12.1.3. e 12.1.4. do subitem acima deste Termo de Referência, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);

12.2.3. **Declaração de inidoneidade para licitar e contratar**, quando praticadas as condutas descritas nas alíneas 12.1.5., 12.1.6., 12.1.7. e 12.1.8. do subitem acima deste Termo de Referência, bem como nas alíneas 12.1.2., 12.1.3. e 12.1.4., que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 2021).

12.2.4. **Multa**:

12.2.4.1. **moratória**, nos casos de atrasos injustificados no início da prestação dos serviços, de 0,5% (cinco décimos por cento) ao dia, sobre o valor da contratação, até o limite de 20 (vinte) dias;

12.2.4.1.1. O atraso superior a 15 (quinze) dias, na infração prevista neste subitem, autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.

12.2.4.2. **moratória**, nos casos de atrasos injustificados no cumprimento dos prazos estabelecidos para a execução dos serviços, de 0,5% (cinco décimos por cento) ao dia, sobre o valor da contratação, até o limite de 30 (trinta) dias;

12.2.4.2.1. O atraso superior a 20 (vinte) dias, na infração prevista neste subitem, autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.

12.2.4.3. **moratória** de 1% (um por cento) por dia de atraso injustificado sobre o valor total da garantia, limitado a 30 (trinta) dias, pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia.

12.2.4.4.1. O atraso superior a 30 (trinta) dias, nas infração prevista no subitem 12.2.4.3., autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.

12.2.4.4. **compensatória** de 25% (vinte e cinco por cento) sobre o valor do contrato, em caso de inexecução total do objeto;

12.2.4.5. **compensatória** de 25% (vinte e cinco por cento) sobre o saldo do contrato, em caso de inexecução parcial dele, que também estará configurada quando:

12.2.4.5.1. a contratada deixar de regularizar as suas condições de habilitação exigidas na licitação, no prazo determinado pela Fiscalização;

12.3. A aplicação das sanções previstas neste Termo de Referência 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)

12.4. Todas as sanções previstas neste Termo de Referência poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133, de 2021).

12.4.1. 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).

12.4.2. A Administração poderá, mediante despacho fundamentado, suspender a aplicação da penalidade de multa nos casos em que o valor for considerado irrisório.

12.4.2.1. Será considerado irrisório valor inferior a R$ 160,00 (cento e sessenta reais).

12.4.2.2. No caso de reincidência, mesmo que o valor da multa seja irrisório, a penalidade deverá ser aplicada cumulativamente com os efeitos e o valor de multa cuja exigibilidade tenha sido suspensa anteriormente.

12.4.2.3. Para efeito de enquadramento como valor irrisório, deverá ser considerado, individualmente, cada evento incidente sobre o mesmo fato gerador da obrigação que resulte em aplicação da respectiva penalidade.

12.4.2.4. Caso não ocorra a reincidência nos últimos doze meses, contados a partir da primeira ocorrência, ou a vigência contratual encerre antes desse prazo, a multa suspensa deve ser convertida na penalidade de advertência.

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

12.4.4. 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.

12.5. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa à contratada, 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.

12.6. Na aplicação das sanções serão considerados (art. 156, §1º, da Lei nº 14.133, de 2021):

12.6.1. a natureza e a gravidade da infração cometida;

12.6.2. as peculiaridades do caso concreto;

12.6.3. as circunstâncias agravantes ou atenuantes;

12.6.4. os danos que dela provierem para o Contratante;

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

12.7. 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).

12.8. 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 Termo de Referência 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)

12.9. O Contratante deverá, 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)

12.10. 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.

12.11. Para a garantia da ampla defesa e do contraditório, as notificações serão enviadas, mediante Intimação Eletrônica, regulamentada pelo Ato Normativo STM nº 430, de 2020.

13. REAJUSTE

13.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado.

13.1.1. A data do orçamento estimado será informada no Edital.

13.2. Após o interregno de um ano, e independentemente de pedido da contratada, os preços iniciais serão reajustados, mediante a aplicação, pelo Contratante, do índice **Índice de Custos de Tecnologia da Informação - ICTI,** mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPE, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

13.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

13.4. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o Contratante pagará à contratada a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

13.5. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

13.6. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

13.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

13.8. O reajuste será realizado por apostilamento.

14. ADEQUAÇÃO ORÇAMENTÁRIA

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

14.1.1. A contratação será atendida pela seguinte dotação:

14.1.1.1. Gestão/Unidade: **DITIN**

14.1.1.2. Programa de Trabalho: SEG0

14.1.1.3. Elemento de Despesa: 3.3.90.40

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

15. ALTERAÇÕES

15.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021.

15.2. A contratada é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato, e, no caso de reforma de edifício ou de equipamento, o limite para acréscimos será de 50% (cinquenta por cento).

15.3. As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial do contrato.

15.4. 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).

15.5. 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.

16. EXTINÇÃO CONTRATUAL

16.1. O contrato será extinto quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes.

16.1.1. O contrato poderá ser extinto antes do prazo nele fixado, sem ônus para o Contratante, quando este não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

16.1.2. A extinção nesta hipótese ocorrerá na próxima data de aniversário do contrato, desde que haja a notificação da contratada pelo Contratante nesse sentido com pelo menos 2 (dois) meses de antecedência desse dia.

16.1.3. Caso a notificação da não-continuidade do contrato de que trata este subitem ocorra com menos de 2 (dois) meses da data de aniversário, a extinção contratual ocorrerá após 2 (dois) meses da data da contratação.

16.2. A contratação poderá ser extinta 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.

16.2.1. Ainda que a extinção unilateral não seja analisada de forma concomitante com a apuração de responsabilidade para fins de aplicação de penalidade administrativa, serão resguardados os seguintes prazos para a contratada no processo de extinção.

16.2.1.1. prazo de 15 (quinze) dias úteis, contado da data da intimação da contratada, para exercício da ampla defesa e do contraditório;

16.2.1.2. prazo de 15 (quinze) dias úteis, contado da data da intimação da contratada, para alegações finais, nos casos de deferimento de pedido de produção de novas provas ou de juntada de provas julgadas indispensáveis para a decisão de extinção unilateral.

16.2.1.3. prazo de 3 (três) dias úteis, contado da data da intimação da contratada, para recurso administrativo (art. 165, I, e), da Lei nº 14.133, de 2021).

16.2.1.4. Para a garantia da ampla defesa e do contraditório, as notificações serão envidas, mediante Intimação Eletrônica, regulamentada pelo Ato Normativo STM nº 430, de 2020.

16.2.2. Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei.

16.2.3. A alteração social ou a modificação da finalidade ou da estrutura da da empresa não ensejará a extinção se não restringir sua capacidade de concluir a contratação.

16.4.3.1. Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizada a alteração subjetiva.

16.3. A extinção, sempre que possível, será precedida:

16.3.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

16.3.2. Relação dos pagamentos já efetuados e ainda devidos;

16.3.3. Indenizações e multas.

16.4. A extinção da contratação 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).

16.5. O Contratante poderá ainda:

16.5.1. nos casos de obrigação de pagamento de multa pela contratada, reter a garantia prestada a ser executada, conforme legislação que rege a matéria;

16.5.2. nos casos em que houver necessidade de ressarcimento de prejuízos causados à Administração, nos termos do inciso IV do art. 139 da Lei nº 14.133, de 2021, reter os eventuais créditos existentes em favor da contratada decorrentes da contratação.

16.6. A contratação poderá ser extinta caso se constate que a contratada 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 nº 14.133, de 2021).

16.7. A contratação poderá ser extinta caso se constate que a pessoa jurídica contratada tem 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 administrativass, 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 art. 2º, inciso VI, da Resolução CNJ nº 07, de 2005;

16.7.1. A vedação constante do subitem anterior se estende às contratações cujo procedimento licitatório tenha sido deflagrado quando os magistrados e servidores geradores de incompatibilidade estavam no exercício dos respectivos cargos e funções, assim como às licitações iniciadas até 6 (seis) meses após a desincompatibilização.

16.8. A contratação poderá ser extinta caso se constate que a pessoa jurídica contratada contratou empregados que sejam cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de ocupantes de cargos de direção e de assessoramento, de ministros ou juízes da respectiva Auditoria contratante, conforme art. 3º da Resolução CNJ nº 07, de 2005, seguindo o definido no Ato Normativo STM nº 640, de 2023 (3205183).

17. CASOS OMISSOS

17.1. Os casos omissos serão decididos pelo Contratante, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

18. FORO

18.1. Fica eleito o Foro da Justiça Federal em Brasília, Seção Judiciária do Distrito Federal para dirimir os litígios que decorrerem da execução desta contratação que não puderem ser compostos pela conciliação, conforme art. 92, §1º, da Lei nº 14.133, de 2021.

19. EQUIPE PARA A FISCALIZAÇÃO DO CONTRATO

GESTOR	**FISCAL DEMANDANTE**	**FISCAL TÉCNICO**	**FISCAL ADMINISTRATIVO**
WILSON MARQUES DE SOUZA FILHO Coordenador	**MARCIO COELHO MARQUES** Chefe de Seção	**CLAUDIO DE OLIVEIRA MELO** Assistente III	**PAULO CESAR CAIXETA** Assistente III
GESTOR	**FISCAL DEMANDANTE SUBSTITUTO**	**FISCAL TÉCNICO SUBSTITUTO**	**FISCAL ADMINISTRATIVO**
WILSON MARQUES DE SOUZA FILHO Coordenador	**CLAUDIO DE OLIVEIRA MELO** Assistente III	**MARCIO COELHO MARQUES** Chefe de Seção	**SIDNEI TIVES DE SOUZA** Chefe de Seção

20. EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

INTEGRANTE DEMANDANTE

WILSON MARQUES DE SOUZA FILHO
Coordenador

INTEGRANTE TÉCNICO

MARCIO COELHO MARQUES
Chefe de Seção

INTEGRANTE ADMINISTRATIVO

LUIS GUSTAVO COSTA REIS
Analista Judiciário

AUTORIDADE MÁXIMA DA ÁREA DE TIC

IANNE CARVALHO BARROS
Diretor de Tecnologia da Informação

ANEXO I - REQUISITOS TÉCNICOS E SLA

1.1. Requisitos necessários:

1.2. Contratação de empresa especializada em segurança cibernética para prestação de Serviços Gerenciado de Segurança da Informação, composta por equipamento para proteção de perímetro do tipo NGFW com SD-WAN, suporte e garantia pelo período de 60 meses.

1.3. Caracterização da demanda

1.3.1. Definição e Especificação das Necessidades

A necessidade primordial que impulsiona esta contratação é a proteção dos ativos de informação e a garantia da continuidade dos serviços jurisdicionais da Justiça Militar da União (JMU)1111. Em um cenário de crescente sofisticação dos ataques cibernéticos, a infraestrutura atual de segurança de perímetro, embora funcional, necessita de uma modernização tecnológica e de um novo modelo de gestão para fazer frente às ameaças complexas e persistentes

A necessidade de quatro tipos distintos de equipamentos para proteção de perímetro do tipo NGFW com SD-WAN (Tipo I, II, III, e IV) decorre da diversidade de requisitos de desempenho, capacidade e conectividade demandados pelos diferentes pontos da rede da Contratante, a Justiça Militar da União (JMU).

1. Tipo I (Concentrador): São necessárias 2 unidades que atuarão como concentradores.

2. Tipo II (Unidade Remota): É necessária 1 unidade. Conforme sua especificação, esta unidade será utilizada na garagem do STM, onde está localizado o backup, exigindo interfaces de rede de 10Gbps ou superior.

3. Tipo III (Unidades Remotas): São necessárias 3 unidades. Estas serão instaladas nas Auditorias do Rio de Janeiro, São Paulo e Brasília. Possuem requisitos de desempenho e capacidade inferiores ao Tipo II, mas ainda significativos.

4. Tipo IV (Unidades Remotas): São necessárias 12 unidades. Estas serão instaladas nas demais Auditorias. Representam o equipamento com os requisitos de desempenho e capacidade mínimos.

A divisão em tipos otimiza o custo da solução ao dimensionar os equipamentos conforme a demanda real de cada localidade, ao invés de usar um modelo único que seria superdimensionado para a maioria das unidades ou subdimensionado para o concentrador e o site de backup.

As necessidades tecnológicas e de negócio que motivam esta contratação são:

· **Proteção Abrangente de Perímetro:** Implementar uma barreira de segurança avançada na fronteira da rede para inspecionar, controlar e proteger o tráfego de entrada e saída contra uma vasta gama de ameaças, incluindo malware, invasões e ataques de dia zero.

· **Otimização da Conectividade e Desempenho de Rede:** Utilizar a tecnologia SD-WAN para gerenciar múltiplos links de rede de forma inteligente, garantindo a qualidade de serviço (QoS) para aplicações críticas, a resiliência da conexão e a otimização do uso da largura de banda.

· **Gerenciamento Centralizado e Eficiente:** A necessidade de uma solução que permita o gerenciamento unificado de todas as funcionalidades de segurança e SD-WAN, simplificando a administração, monitoramento e geração de relatórios.

· **Disponibilidade e Continuidade:** Garantir que os serviços de segurança e conectividade permaneçam operacionais, mesmo diante de falhas ou incidentes, com mecanismos de redundância e alta disponibilidade.

· **Conformidade e Governança:** Atender às políticas de segurança da informação e proteção de dados da instituição, bem como às normativas do Conselho Nacional de Justiça (CNJ), especialmente a Resolução CNJ nº 396/2021 (Estratégia Nacional de Segurança Cibernética do Poder Judiciário).

· **Suporte Especializado e Dedicado:** Contar com profissionais qualificados e dedicados para a instalação, configuração, operação assistida, resolução de problemas e ajuste de políticas, liberando a equipe interna de TI para outras atividades estratégicas.

1.3.2. Definição e Especificação de Requisitos

Os requisitos técnicos e funcionais detalhados a seguir foram formulados para atender integralmente às necessidades descritas. Eles representam o conjunto de capacidades, desempenhos e funcionalidades que a solução contratada deverá obrigatoriamente possuir para ser considerada tecnicamente viável e aderente aos objetivos estratégicos do STM.

1.3.3. Requisitos Funcionais

Os requisitos a seguir são transcritos e justificados com base na estrutura do documento de Especificação Técnica Detalhada.

1.3.3.1. Requisitos de arquitetura tecnológica (Configuração):

1.3.3.1.1. Características Gerais do Serviço Gerenciado

Esta seção define o escopo e as condições gerais da prestação de serviço, assegurando transparência, segurança jurídica e o alinhamento com as necessidades de gestão do STM.

a) Requisito: As licenças (subscrição) dos softwares que compõem os itens 1, 2, 3 e 4 do grupo 1 devem ser emitidas no nome da contratante.

Justificativa: Garante a posse legal e o direito de uso dos ativos de software pelo STM. Essa condição é fundamental para a gestão de ativos de TIC, conformidade em auditorias e, crucialmente, para evitar a dependência excessiva (vendor lock-in), assegurando a continuidade operacional caso haja uma futura troca do prestador de serviço.

b) Requisito: Sobre os itens 1, 2, 3 e 4 do grupo 1, especificar os custos envolvidos com licenças de softwares e outros custos (pessoas).

Justificativa: Promove a transparência na composição de preços da proposta. A segregação de custos permite ao STM avaliar a economicidade de cada componente do serviço (o custo do licenciamento vs. o custo do serviço gerenciado/pessoal), facilitando a análise comparativa com o mercado e o planejamento orçamentário para futuras renovações ou expansões.

c) Requisito: Caso seja necessário substituir licenças equivalentes durante a vigência do contrato, isso deverá ocorrer sem qualquer ônus para a contratante8.

Justificativa: Mitiga o risco tecnológico e financeiro associado ao ciclo de vida dos produtos. Fabricantes podem descontinuar linhas de produtos ou modelos de licenciamento. Esta cláusula protege o investimento do STM, garantindo que o nível de serviço e as funcionalidades contratadas serão mantidos com tecnologia equivalente ou superior sem custos adicionais imprevistos.

d) Requisito: Os equipamentos de proteção de perímetro com SD-WAN que compõem o serviço devem ser novos e sem uso anterior, em linha de produção e fornecidos em sua versão mais atualizada.

Justificativa: Assegura que o STM receberá uma solução tecnológica de ponta, com o máximo de vida útil, garantia integral do fabricante e as mais recentes correções de segurança e funcionalidades. Isso evita o recebimento de equipamentos recondicionados ou próximos do fim de vida (End-of-Life), que representam maior risco de falhas e menor janela de suporte.

e) Requisito: Fornecimento de monitoração e gerenciamento através de SOC/NOC para todos os equipamentos, com a CONTRATADA sendo responsável por implementar e gerenciar as políticas de segurança definidas pelo cliente10.

Justificativa: Este é o cerne do modelo de "Serviço Gerenciado". Ele transfere a responsabilidade da operação, monitoramento 24x7 e resposta inicial a incidentes para a contratada, que possui um Centro de Operações de Segurança/Rede (SOC/NOC). Isso libera a equipe interna da DITIN de tarefas operacionais intensivas, permitindo foco em ações estratégicas, ao mesmo tempo que garante vigilância contínua e especializada do ambiente.

f) Requisito: Fornecimento de um profissional sênior, dedicado de forma exclusiva e contínua, para gerenciamento e administração de todos os serviços e equipamentos.

Justificativa: Dada a criticidade e complexidade da solução, um ponto focal de alta especialização é indispensável. A dedicação exclusiva garante que o profissional terá um conhecimento profundo e contextualizado do ambiente do STM, resultando em maior agilidade no suporte avançado (Nível 2 e 3), proatividade na otimização de políticas e eficácia na resolução de problemas complexos, servindo como uma extensão qualificada da equipe da COTEC.

1.3.3.2. Especificações Técnicas Mínimas dos Equipamentos

1.3.3.2.1. Equipamento Tipo I (Concentrador - Sede/Data Center)

a) Requisito: Desempenho de Next Generation Firewall de 19 Gbps, 8 Gbps com todas as funcionalidades de segurança ativas, e 3.6 Gbps para tráfego com inspeção SSL/TLS.

Justificativa: Estas métricas de desempenho são críticas para o Data Center, que concentra todo o tráfego da JMU. O alto desempenho garante a inspeção profunda de todo o tráfego, inclusive o criptografado (onde ameaças se ocultam), sem criar gargalos que afetem a performance dos sistemas judiciais e administrativos.

b) Requisito: Suporte a 240.000 novas conexões/segundo e 3.000.000 de conexões simultâneas.

Justificativa: A alta taxa de novas conexões é vital para suportar picos de acesso. O alto número de conexões simultâneas é necessário para manter a estabilidade de todas as sessões ativas dos usuários, sistemas e serviços.

c) Requisito: Fonte de alimentação redundante.

Justificativa: Requisito básico de alta disponibilidade. Evita que a falha de um componente de energia cause a interrupção completa do acesso à rede, garantindo a continuidade dos serviços.

d) Requisito: Alta densidade de interfaces de rede (8x 10/100/1000 Base-T, 8x 10Gbps SFP+, 4x 25Gbps SFP28).

Justificativa: Necessário para a interconexão com a rede de alta velocidade do Data Center do STM, incluindo switches de core, servidores e outros equipamentos, garantindo uma arquitetura moderna e escalável.

e) Requisito: Possuir interface dedicada e física para gerenciamento do equipamento fora de banda (Out-of-Band Management). Essa interface deve ser um canal de gerenciamento que funcione mesmo quando o dispositivo não responde. Não sendo permitido qualquer tipo de configuração via software para esta função.

Justificativa : Este requisito é um pilar fundamental para a resiliência, a recuperabilidade e a gestão segura da infraestrutura crítica de segurança do STM. A exigência de uma interface de gerenciamento física e verdadeiramente fora de banda vai além de uma simples conveniência administrativa; ela é uma salvaguarda essencial contra cenários de falha que poderiam comprometer toda a operação da Justiça Militar da União.

1. Garantia de Continuidade Operacional e Resiliência em Cenários de Falha Crítica: O firewall de perímetro é um dos ativos mais críticos da rede. Uma falha neste equipamento resulta na interrupção total da comunicação, paralisando serviços essenciais como o e-Proc/JMU. A interface fora de banda, por ser um canal físico e eletronicamente independente, funciona como uma "UTI" para o equipamento, provendo um caminho alternativo e direto para a equipe de TI realizar ações de emergência, mesmo que o "cérebro" principal do equipamento esteja incapacitado.

2. Redução Drástica do Tempo Médio de Reparo (MTTR): Sem uma interface OOB, a única solução para uma falha crítica é o deslocamento físico de um técnico ao Data Center, processo que pode levar horas. Com a gerência OOB, o Tempo Médio de Reparo (MTTR) é reduzido para minutos, pois a equipe da DITIN pode acessar a console de emergência de forma remota e imediata (24x7) para iniciar a recuperação.

3. Segurança e Confiabilidade da Gestão do Dispositivo: A exigência de ser física e dedicada garante que o canal de recuperação seja verdadeiramente independente do sistema operacional principal, que pode estar travado. Adicionalmente, este canal é inerentemente mais seguro, pois fica isolado em uma rede de gerenciamento restrita, protegido de ameaças da rede principal.

f) Requisito : Arquitetura modular de interfaces de rede.

Justificativa: Garante a proteção do investimento e a flexibilidade da solução a longo prazo. Permite que o firewall se adapte a futuras atualizações da rede (ex: migração para 40Gbps) apenas com a troca de um módulo, em vez de todo o equipamento, promovendo economia e escalabilidade.

1.3.3.2.2. Equipamento Tipo II (Unidades Remotas de Grande Porte)

a) Requisito: Desempenho de Next Generation Firewall de 5 Gbps e 1.5 Gbps com todas as funcionalidades de segurança ativas.

Justificativa: Adequado para as maiores localidades remotas da JMU, garantindo que tenham capacidade de processamento para aplicar todas as políticas de segurança ao tráfego local e às conexões com a sede, sem comprometer a performance para os usuários.

b) Requisito: Suporte a 50.000 novas conexões/segundo e 300.000 conexões simultâneas.

Justificativa: Capacidade dimensionada para o volume de usuários e serviços dessas unidades, garantindo estabilidade e resposta rápida durante picos de uso.

1.3.3.2.3. Equipamento Tipo III (Unidades Remotas de Médio Porte)

a) Requisito: Desempenho de Next Generation Firewall de 3.2 Gbps e 1.5 Gbps com todas as funcionalidades de segurança ativas.

Justificativa: Perfil de desempenho ajustado para localidades de médio porte. Assegura a aplicação integral do mesmo nível de segurança do Data Center, porém com um hardware dimensionado para a realidade local, em conformidade com o princípio da economicidade.

b) Requisito: Suporte a 50.000 novas conexões/segundo e 300.000 conexões simultâneas.

Justificativa: Garante a fluidez e estabilidade das operações para o número de usuários e sistemas presentes nessas unidades.

1.3.3.2.4. Equipamento Tipo IV (Unidades Remotas de Pequeno Porte)

a) Requisito: Desempenho de Next Generation Firewall de 1.3 Gbps e 660 Mbps com todas as funcionalidades de segurança ativas.

Justificativa: O dimensionamento mais enxuto atende com eficiência e menor custo às necessidades das menores localidades da JMU. O mais importante é que, apesar do porte, o equipamento deve prover o conjunto completo de funcionalidades de segurança, garantindo uma postura de segurança uniforme em toda a instituição.

b) Requisito: Suporte a 20.000 novas conexões/segundo e 175.000 conexões simultâneas.

Justificativa: Capacidade suficiente para garantir a performance e a estabilidade da rede para o perfil de uso dessas unidades.

1.3.3.2.5. Especificações Técnicas de Funcionalidades (Comum a todos os equipamentos)

a) Requisito: Reconhecer pelo menos 3.000 aplicações diferentes, independente de porta e protocolo, e controlar funções específicas dentro da aplicação.

Justificativa: Essencial para implementar políticas de segurança eficazes na era da nuvem. Permite à DITIN controlar o uso de aplicações para mitigar riscos de vazamento de dados e perda de produtividade, sem precisar bloquear serviços inteiros que possam ter uso legítimo para o negócio.

b) Requisito: Possuir módulo de IPS com no mínimo 7.000 assinaturas e referência cruzada com CVE.

Justificativa: O IPS protege ativamente a rede contra tentativas de exploração de vulnerabilidades conhecidas. A referência ao CVE é crucial, pois permite correlacionar um alerta de ataque a uma vulnerabilidade específica, facilitando a gestão de riscos e a priorização de correções.

c) Requisito: Medir parâmetros de rede como jitter, perda de pacotes e latência em tempo real e redistribuir o tráfego de forma inteligente entre os links (SD-WAN).

Justificativa: Fundamental para garantir a qualidade de serviços em tempo real, como sessões de julgamento por videoconferência. O SD-WAN monitora a "saúde" dos links e desvia o tráfego crítico para o de melhor performance, garantindo uma experiência de uso fluida.

d) Requisito: Suportar VPN (Site-to-Site e Client-to-Site) com múltiplos métodos de autenticação, incluindo integração com provedores de identidade via SAML.

Justificativa: Essencial para o trabalho remoto seguro e para a interligação das unidades. O suporte a SAML é um requisito moderno que permite a implementação de Autenticação Multifator (MFA), elevando drasticamente a segurança do acesso remoto.

e) Requisito: Analisar e bloquear ameaças não conhecidas (zero-day) em tempo real, utilizando um ambiente sandbox em nuvem do próprio fabricante.

Justificativa: Malwares modernos, especialmente ransomware, são projetados para não serem detectados por assinaturas. O sandboxing analisa o comportamento do arquivo em um ambiente seguro antes que ele chegue ao usuário, sendo a defesa mais eficaz contra este tipo de ataque.

f) Requisito: Centralizar a administração de regras, políticas e logs de todos os equipamentos em uma única interface, com recursos avançados de pesquisa e correlação de eventos.

Justificativa: Indispensável para a eficiência operacional, consistência da segurança e capacidade de resposta a incidentes. Permite gerenciar dezenas de dispositivos como um só e facilita a investigação de incidentes ao consolidar e correlacionar informações de múltiplas fontes em um único local.

1.3.3.3. Requisitos de Manutenção:

A contratação prevê a prestação de Serviços Gerenciado de Segurança da Informação, o que implica que a empresa contratada será responsável pela manutenção e resolução de problemas. Os requisitos de manutenção incluem:

a) Serviços de manutenção preventiva, corretiva, adaptativa e evolutiva (melhoria funcional) para todos os equipamentos e softwares que compõem a solução, sem ônus adicional para a Contratante.

b) A forma como será conduzida a manutenção, acionamento da garantia e a comunicação entre as partes envolvidas deverão ser claramente definidas em Acordo de Nível de Serviço (SLA).

c) Resolução de qualquer problema nas licenças e serviços descritos no documento de especificação técnica.

1.3.3.4. Requisitos de projeto e de implementação:

- A Contratada será responsável por implementar e gerenciar as políticas de segurança definidas pelo cliente.
- Fornecimento de equipamentos novos e sem uso anterior.
- A solução ofertada deverá estar em linha de produção, sem previsão de encerramento de fabricação, na data de entrega da proposta.
- O licenciamento deverá ser fornecido em sua versão mais atualizada.
- As licenças (subscrição) dos softwares que compõem os itens 1, 2, 3 e 4 do grupo 1 devem ser emitidas no nome da contratante.
- Caso seja necessário substituir licenças equivalentes durante a vigência do contrato, isso deverá ocorrer sem qualquer ônus para a contratante.
- Apoio técnico especializado nas fases de instalação, configuração, integração e ativação dos equipamentos NGFW com SD-WAN.
- Elaboração de planos de implantação e documentação técnica.
- Apoio técnico durante o período de sustentação e operação assistida da solução, com atuação pró-ativa na resolução de problemas.

1.3.3.5. Requisitos de implantação:

- O processo de disponibilização da solução em ambiente de produção deverá ser planejado em conjunto com a Contratante, minimizando impactos nas operações.
- A Contratada será responsável pela implementação e gestão das políticas de segurança, incluindo regras de firewall, IPS, Antivírus/Anti-malware, filtro URL, controle de aplicações e SD-WAN, conforme as políticas de segurança estabelecidas.
- Configuração de rotas avançadas de acordo com a demanda do cliente.
- Suporte técnico especializado para integração do equipamento para proteção de perímetro com outras soluções de segurança e redes.

1.3.3.6. Requisitos de experiência profissional

- A Contratada deverá fornecer, no mínimo, 01 (um) profissional sênior, dedicado para gerenciamento e administração de todos os serviços e equipamentos fornecidos neste edital.
- Este profissional será alocado de forma **exclusiva e contínua**, sendo responsável por atividades como apoio técnico especializado nas fases de instalação, configuração, integração e ativação; atendimento técnico dedicado de Nível 2 e 3 (troubleshooting avançado, tunning de políticas, análise de desempenho, gestão de conectividade dinâmica); elaboração de planos de implantação, documentação técnica e relatórios; suporte na criação e ajuste de políticas de segurança, regras de inspeção profunda (DPI), controle de aplicações, filtragem de conteúdo, VPNs e segmentação de tráfego via SD-WAN; e apoio técnico durante o período de sustentação e operação assistida, com atuação pró-ativa na resolução de problemas.

1.3.3.6.1. Requisitos obrigatórios para o profissional dedicado:

a) Experiência mínima de 4 (quatro) anos, comprovada, na atuação direta com soluções de NGFW, incluindo atividades de implantação, configuração, troubleshooting e suporte técnico.

- A comprovação da experiência deverá ser feita mediante apresentação de currículo atualizado e detalhado, cópias de contratos, atestados de capacidade técnica ou declarações emitidas por empresas públicas ou privadas, com descrição das atividades desempenhadas e identificação da tecnologia envolvida.

b) Conhecimento técnico avançado na solução ofertada.

c) A Contratada deverá apresentar declaração formal garantindo a alocação dedicada deste profissional durante todas as fases do projeto, inclusive suporte pós-implantação.

d) O profissional deverá estar disponível para atendimento remoto e presencial (quando necessário), respeitando os prazos de SLA definidos neste Termo de Referência.

e) O profissional técnico designado pela Contratada deverá, **sempre que solicitado pela CONTRATANTE**, realizar suas atividades de forma **presencial nas dependências da CONTRATANTE**, em **horário comercial (das 12h às 19h, em dias úteis)**, **sem quaisquer ônus adicionais** à Contratante.

f) O profissional dedicado deverá seguir todas as políticas internas de segurança da informação da Contratante.

g) A Contratante terá acesso direto ao profissional dedicado através de uma linha direta (hotline), permitindo comunicação imediata e eficaz.

Caso necessário, a Contratante poderá acionar outros recursos do suporte da contratada para a resolução de problemas.

Justificativa: A complexidade da solução de NGFW com SD-WAN e a criticidade dos serviços de segurança da informação exigem um profissional com experiência comprovada e certificações específicas do fabricante para garantir a correta implantação, configuração e sustentação, minimizando riscos operacionais e de segurança. A dedicação e o atendimento presencial garantem agilidade e proximidade com a equipe de TI da Contratante.

1.3.3.7. Requisitos de formação da equipe

Os requisitos de formação da equipe estão abrangidos nos requisitos de experiência profissional e certificações específicas exigidas para o profissional sênior dedicado[57]. A formação acadêmica e técnica específica para atuar com as tecnologias de segurança cibernética e SD-WAN é implícita nas certificações e experiência.

1.3.3.8. Acordo de Nível de Serviço (SLA)

1.3.3.8.1. Objetivo

Este Acordo de Nível de Serviço (SLA) tem como objetivo definir os níveis mínimos de desempenho, disponibilidade e qualidade para os "Serviços Gerenciados de Segurança da Informação"[1], objeto desta contratação. Ele estabelece as métricas, os tempos de resposta e solução para incidentes e requisições de serviço, bem como as penalidades aplicáveis em caso de descumprimento, assegurando que o STM receba um serviço de excelência, compatível com a criticidade de suas operações.

1.3.3.8.2. Definições

Para os fins deste SLA, aplicam-se as seguintes definições:

a) Incidente: Qualquer evento não planejado que cause, ou possa causar, uma interrupção ou redução na qualidade do serviço.

b) Requisição de Serviço: Uma solicitação formal para uma mudança padrão, como a criação de uma nova regra de firewall, a geração de um relatório específico ou uma consulta de configuração que não se origine de uma falha.

c) Horário Comercial (HC): De segunda a sexta-feira, das 09:00 às 19:00, horário de Brasília-DF, exceto feriados nacionais e do Distrito Federal.

d) Tempo de Resposta: O intervalo de tempo entre a abertura do chamado pelo STM (ou a detecção proativa pela CONTRATADA) e o início efetivo do atendimento por um analista qualificado, com a devida comunicação ao STM.

e) Tempo de Solução de Contorno: O intervalo de tempo para o restabelecimento do serviço por meio de uma solução temporária (workaround) que mitigue o impacto do incidente.

f) Tempo de Solução Definitiva: O intervalo de tempo para a resolução completa e definitiva da causa raiz do incidente.

1.3.3.8.3. Classificação de Prioridade de Incidentes

Todo incidente será classificado conforme a tabela abaixo, em comum acordo entre o STM e a CONTRATADA. Em caso de divergência, prevalecerá a classificação do STM.

Prioridade	Descrição	Exemplos
P1 - Crítica	Indisponibilidade total do serviço em um ou mais equipamentos do tipo I (Concentrador); falha que afeta a comunicação de múltiplas localidades; violação de segurança grave em andamento; indisponibilidade de sistema crítico (e-Proc/JMU) comprovadamente causada por falha na solução.	Queda completa dos firewalls da sede; falha total do acesso VPN para todos os usuários; detecção de um ataque de ransomware ativo na rede.

P2 - Alta	Degradação severa do desempenho do serviço; indisponibilidade de uma funcionalidade de segurança crítica (ex: IPS, Filtro Web); falha de um dos links gerenciados pelo SD-WAN; falha em um equipamento de localidade remota causando indisponibilidade local.	Lentidão extrema na rede afetando todos os usuários; falha no módulo de antivírus de gateway; queda de um dos links de internet da sede.
P3 - Média	Degradação parcial do serviço com baixo impacto; falha que afeta um pequeno grupo de usuários ou um serviço não crítico; falha em uma política de segurança específica.	Uma regra de firewall específica não está funcionando; falha no agendamento de um relatório; dificuldade de acesso para um único usuário.
P4 - Baixa	Incidente sem impacto perceptível no serviço; solicitação de informação ou dúvida sobre o funcionamento da solução; otimização de regra sem urgência.	Esclarecimento sobre uma funcionalidade; log de evento informativo que gerou dúvida.

1.3.3.8.4. Métricas de Nível de Serviço para Incidentes

A CONTRATADA deverá cumprir os seguintes prazos, contados a partir da abertura do chamado:

Prioridade	Canal de Acionamento	Horário de Cobertura	Tempo de Resposta (Máximo)	Tempo de Solução de Contorno (Máximo)	Tempo de Solução Definitiva (Máximo)
P1 - Crítica	Telefone (Hotline) [2] / E-mail	24x7x365	15 minutos	4 horas	24 horas
P2 - Alta	Telefone (Hotline) / E-mail	24x7x365	30 minutos	8 horas	3 dias úteis
P3 - Média	Portal Web / E-mail	Horário Comercial	1 hora	N/A	5 dias úteis
P4 - Baixa	Portal Web / E-mail	Horário Comercial	2 horas	N/A	10 dias úteis

1.3.3.8.5. Métricas de Nível de Serviço para Requisições de Serviço

Tipo de Requisição	Prazo para Conclusão (Máximo)
Alteração de política de segurança (Crítica/Emergencial)	4 horas (24x7)
Alteração de política de segurança (Padrão)	2 dias úteis
Geração de relatório customizado	3 dias úteis
Consulta técnica ou esclarecimento de dúvida	1 dia útil

1.3.3.8.6. Nível de Disponibilidade do Serviço

a) Disponibilidade Mínima Mensal: A solução, considerando os clusters de alta disponibilidade (equipamentos Tipo I), deverá ter uma disponibilidade mínima de 99,9% ao mês.

b) Cálculo da Disponibilidade: A disponibilidade será calculada pela fórmula:

Disponibilidade(%) = (1 - Tempo Total de Indisponibilidade em Minutos/Total de Minutos no Mês) X 100

c) Janelas de Manutenção: Manutenções programadas que exijam indisponibilidade do serviço deverão ser previamente acordadas com o STM com no mínimo 5 (cinco) dias úteis de antecedência e realizadas, preferencialmente, em finais de semana ou fora do horário de expediente. Janelas de manutenção acordadas não serão computadas como tempo de indisponibilidade.

1.3.3.8.7. Penalidades por Descumprimento do SLA

Infração	Percentual de Glosa
Descumprimento do Tempo de Resposta (P1 ou P2)	2% por evento
Descumprimento do Tempo de Solução de Contorno (P1)	5% por evento, por hora de atraso
Descumprimento do Tempo de Solução de Contorno (P2)	3% por evento, por hora de atraso
Disponibilidade Mensal entre 99,0% e 99,89%	10%
Disponibilidade Mensal entre 98,0% e 98,99%	15%
Disponibilidade Mensal abaixo de 98,0%	20%

- **Limite de Glosa:** O somatório das glosas aplicadas em um mês não poderá exceder 30% do valor da fatura mensal. A reincidência contumaz no descumprimento do SLA poderá ensejar a abertura de processo administrativo para rescisão contratual por inexecução.

1.3.3.8.8. Relatórios de Nível de Serviço

A CONTRATADA deverá fornecer ao STM, até o 5º dia útil de cada mês, um relatório detalhado contendo o desempenho do serviço no mês anterior. O relatório deve incluir, no mínimo:

a) Lista de todos os incidentes e requisições de serviço, com seus respectivos horários de abertura, resposta e solução.

b) Cálculo do cumprimento de todas as métricas de SLA.

c) Cálculo da disponibilidade mensal do serviço.

d) Análise de causa raiz para todos os incidentes de prioridade P1 e P2.

e) Sumário executivo das atividades realizadas pelo profissional dedicado.

1.3.3.9. Requisitos Temporais:

A prestação de serviços e a garantia dos equipamentos deverão ser pelo período de 60 meses.

O contrato vigente encerra-se em dezembro de 2025, sendo crucial que a nova contratação esteja operacional a partir de janeiro de 2026 para garantir a continuidade dos serviços de proteção de perímetro.

1.3.3.10. Requisitos de Segurança da Informação

A CONTRATADA deverá assinar Termo de Sigilo/Confidencialidade, obrigando-se a não realizar, promover, nem incentivar a divulgação de qualquer dado ou informação do ambiente computacional do STM, bem como dos dados ou informações contidas nele sem a prévia autorização.

Os encarregados dos serviços previstos nas respectivas Ordens de Serviço deverão assinar Termo de Confidencialidade antes de iniciar suas atividades junto ao STM.

Observar normativos e todos os procedimentos de segurança necessários e definidos na legislação pertinente e vigente no Poder Judiciário.

Submeter seus recursos técnicos aos regulamentos de segurança e disciplina instituídos pelo ÓRGÃO, durante o tempo de permanência nas suas dependências.

Disponibilizar links seguros para a realização de trabalho remoto, quando couber.

A solução deve prover a segurança cibernética e proteção de dados, conforme recomendações da Política de Segurança Cibernética da JMU e Resolução CNJ nº 396/2021.

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.

1.3.3.11. Requisitos Sociais, Ambientais e Culturais

A CONTRATADA deverá tomar conhecimento do Plano de Logística Sustentável PLS, das Orientações do Controle Interno e demais procedimento do STM, ainda que a natureza dos serviços não se aplique, devidamente justificada pela inexistência de produtos ou atividades que se enquadrem nas condições exigidas nos critérios de Sustentabilidade Ambiental, Social e Econômica.

1.3.3.12. Requisitos Legais

A solução deve estar em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n. 13.709, de 14 de agosto de 2018.

A solução deve atender aos requisitos para o atendimento do protocolo para investigação de ilícitos cibernéticos, conforme os requisitos mínimos de segurança definidos na Resolução CNJ nº 396/2021, que institui a Estratégia Nacional de Segurança Cibernética no âmbito do Poder Judiciário.

1.3.3.13. Demais Requisitos Aplicáveis

Garantir prazos de entrega a fim de evitar penalidades por atrasos.

Desenvolver as atividades necessárias mediante trabalho híbrido (remoto/presencial/híbrido) e nos termos dos padrões de segurança e integridade previstas pelo Poder Judiciário e pelo STM.

A Contratada deverá estar apta a abrir e receber Ordens de Serviço via correio eletrônico, sistema específico de controle de demandas ou, página na internet (WEB) dedicada, em regime 24x7 (24 horas por dia, em todos os sete dias da semana).

Responsabilizar-se pelos materiais, produtos, ferramentas, instrumentos e equipamentos disponibilizados para a execução dos serviços, sejam eles prestados remotamente ou nas instalações do STM, não cabendo ao STM qualquer responsabilidade por perdas decorrentes de roubo, furto ou outros fatos que possam vir a ocorrer.

Promover o afastamento, no prazo máximo de 24 (vinte e quatro) horas após o recebimento da notificação por ofício ou e-mail, de qualquer dos seus recursos técnicos que não correspondam aos critérios de confiança ou que perturbem a ação da equipe de fiscalização do STM.

1.3.3.14. Verificação de Amostra do Objeto

A possibilidade de verificação de amostra, tem previsão no artigo 17, §3º, artigo 41, inciso II, e artigo 42, §2º, todos da Lei nº 14.133, de 2021, e no artigo 12, § 1º da IN SGD/ME nº 94, de 2022. Portanto, como são equipamentos de altos valores, o STM poderá solicitar amostra se assim desejar.

Para fins de aceitação pelo STM, este Órgão poderá solicitar amostra para aferir as funcionalidades dos equipamentos em testes de bancada. Os itens de performance serão comprovados mediante datasheet ou declaração do fabricante em casos excepcionais. Os testes de bancada são destinados, exclusivamente, a dirimir dúvidas dos demais participantes do certamente licitatório, quando suscitadas, sobre as capacidades dos equipamentos que serão entregues pelo participante vencedor do certame. Os testes de bancadas consistirão em:

Aferição da capacidade de throughput de tráfego descriptografado pelo equipamento a ser testado.

Aferição da capacidade de trhoughput de inspeção de tráfego SSL do equipamento a ser testado.

Aferição das especificações técnicas (portas de comunicação, capacidade de processamento, memórias estáticas e volátil) do equipamento a ser testado.

Capacidades do software do equipamento a ser testado.

2. DESCRIÇÃO DA SOLUÇÃO DE TIC

2.1. O objeto é composto pelos seguintes itens:

Grupo	Item	Descrição dos serviços	Unidade de Medida	Quantidade (A)	Valor Unitário (B)	Valor Total para 60 (sessenta) meses (C) = A x B x 60
1	1	Serviço composto por equipamento para proteção de perímetro do tipo NGFW com SD-WAN - Tipo I (Concentrador)	Unidade	2		
	2	Serviço composto por equipamento para proteção de perímetro do tipo NGFW com SD-WAN - Tipo II (Unidades Remotas)	Unidade	1		
	3	Serviço composto por equipamento para proteção de perímetro do tipo NGFW com SD-WAN - Tipo III (Unidades Remotas)	Unidade	3		
	4	Serviço composto por equipamento para proteção de perímetro do tipo NGFW com SD-WAN - Tipo IV (Unidades Remotas)	Unidade	12		
	5	Serviço composto por Gerência centralizada, logs, eventos e relatórios para equipamentos de proteção de perímetro com SD WAN.	Unidade	1		

2.2. Características gerais do serviço:

2.2.1. As licenças (subscrição) dos softwares que compõe os itens 1, 2, 3 e 4 do grupo 1 devem ser emitidas no nome da contratante;

2.2.2. Sobre os itens 1, 2, 3 e 4 do grupo 1, especificar os custos envolvidos com licenças de softwares e outros custos (pessoas);

2.2.3. Caso seja necessário substituir licenças equivalentes durante a vigência do contrato, isso deverá ocorrer sem qualquer ônus para a contratante;

2.2.4. Os serviços deverão contemplar a resolução de qualquer problema nas licenças e serviços descritos neste documento, sem nenhum ônus adicional para a contratante;

2.2.5. Os equipamentos de proteção de perímetro com SD-WAN que compõem o serviço, devem ser novos e sem uso anterior. A solução ofertada deverá estar em linha de produção, sem previsão de encerramento de fabricação, na data de entrega da proposta. O licenciamento deverá ser fornecido em sua versão mais atualizada;

2.2.6. O Serviço prevê o fornecimento de hardware/software para proteção de perímetro com SD-WAN que compõe uma solução segura e robusta totalmente gerenciada que possui as seguintes características:

2.2.6.1. Solução que garante conexões segura por links Internet através de tunelamento VPN - Virtual) entre as localidades de acordo com as demandas específicas da rede;

2.2.6.2. Fornecimento de equipamentos, com no mínimo 3 (três) interfaces WAN e todos os requisitos necessários (HW e SW) para habilitação das funcionalidades de proteção de perímetro com SD-WAN Seguro na rede;

2.2.6.3. Fornecimento de monitoração e gerenciamento através de SOC/NOC para todos os equipamentos fornecidos na solução SD-WAN;

2.2.6.4. A CONTRATADA será responsável por implementar e gerenciar as políticas de segurança definidas pelo cliente, com no mínimo:

2.2.6.4.1. Fornecimento de relatórios customizados relativos ao serviço de Segurança contemplando informações básicas tais como uso, performance, disponibilidade dentre outros;

2.2.6.4.2. Diagnóstico e resolução de problemas de configuração, desempenho e segurança dos equipamentos;

2.2.6.4.3. Análise e implementação de regras de firewall, IPS, Antivírus/Anti-malware, filtro URL, controle de aplicações e SD-WAN, conforme políticas de segurança estabelecidas;

2.2.6.4.4. Monitoramento e resposta a incidentes relacionados ao serviço;

2.2.6.4.5. Avaliação periódica das regras e políticas de firewall, IPS, Antivírus/Anti malware, filtro URL, controle de aplicações e SD-WAN para garantir conformidade com as melhores práticas de segurança;

2.2.6.4.6. Configuração de rotas avançadas de acordo com a demanda do cliente;

2.2.6.4.7. Suporte técnico especializado para integração do equipamento para proteção de perímetro com outras soluções de segurança e redes;

2.2.6.4.8. A CONTRATADA deverá fornecer, no mínimo, 01 (um) profissional sênior, dedicado para gerenciamento e administração de todos os serviços e equipamentos fornecidos neste edital;

2.2.6.4.9. Este profissional será alocado de forma exclusiva e contínua, sendo responsável pelas seguintes atividades técnicas:

2.2.6.4.10. Apoio técnico especializado nas fases de instalação, configuração, integração e ativação dos equipamentos NGFW com SD-WAN;

2.2.6.4.11. Atendimento técnico dedicado à CONTRATANTE, com suporte de Nível 2 e 3, englobando troubleshooting avançado, tunning de políticas de segurança, análise de desempenho e gestão de conectividade dinâmica (SD-WAN);

2.2.6.4.12. Elaboração de planos de implantação, documentação técnica e relatórios periódicos de operação e segurança;

2.2.6.4.13. Suporte na criação e ajuste de políticas de segurança, regras de inspeção profunda (DPI), controle de aplicações, filtragem de conteúdo, VPNs e segmentação de tráfego via SD-WAN;

2.2.6.4.14. Apoio técnico durante o período de sustentação e operação assistida da solução, com atuação pró-ativa na resolução de problemas.

2.2.6.5. Requisitos obrigatórios para o profissional dedicado:

2.2.6.5.1. Experiência mínima de 4 (quatro) anos, comprovada, na atuação direta com soluções de NGFW, incluindo atividades de implantação, configuração, troubleshooting e suporte técnico;

2.2.6.5.2. A comprovação da experiência deverá ser feita mediante apresentação de:

2.2.6.5.2.1. Currículo atualizado e detalhado;

2.2.6.5.2.2. Cópias de contratos, atestados de capacidade técnica ou declarações emitidas por empresas públicas ou privadas, com descrição das

atividades desempenhadas e identificação da tecnologia envolvida;

2.2.6.5.3. Conhecimento técnico avançado na solução ofertada;

2.2.6.5.4. A CONTRATADA deverá apresentar declaração formal garantindo a alocação dedicada deste profissional durante todas as fases do projeto, inclusive suporte pós-implantação;

2.2.6.6. O profissional deverá estar disponível para atendimento remoto e presencial (quando necessário), respeitando os prazos de SLA definidos neste Termo de Referência.

2.2.6.6.1. O profissional técnico designado pela CONTRATADA deverá, sempre que solicitado pela CONTRATANTE, realizar suas atividades de forma presencial nas dependências da CONTRATANTE, em horário comercial (das 12h às 19h, em dias úteis), sem quaisquer ônus adicionais à CONTRATANTE;

2.2.6.7. O profissional dedicado deverá seguir todas as políticas internas de segurança da informação da CONTRATANTE;

2.2.6.8. A CONTRATANTE terá acesso direto ao profissional dedicado através de uma linha direta (hotline), permitindo comunicação imediata e eficaz;

2.2.6.8.1. Caso necessário, a CONTRATANTE poderá acionar outros recursos do suporte da contratada para a resolução de problemas;

2.3. Grupo 1 – ITEM 1 - Serviço composto por equipamento para proteção de perímetro do tipo NGFW com SD-WAN - Tipo I

2.3.1. Características especificas mínimas para equipamento de proteção de perímetro do tipo NGFW com SD-WAN - Tipo I

2.3.1.1. Dimensionamento:

· Desempenho requerido, no mínimo, de Next Generation Firewall: 19 (dezenove) Gbps;

· Deve possuir capacidade de processamento de, no mínimo, 8 (oito) Gbps para tráfego stateful inspection TCP completo, sem amostragem, com as funcionalidades de Next Generation firewall, controle de aplicações, IPS e Anti Malware ativas simultaneamente.

· Deve possuir capacidade de processamento de, no mínimo, 3.6 (três ponto seis) Gbps para tráfego stateful inspection TCP, com funcionalidade de descriptografia e inspeção completa de todos os fluxos, sem amostragem, considerando-se pelo menos 50% de tráfego TLS 1.2 e com todas as funcionalidades habilitadas simultaneamente;

· Desempenho requerido, no mínimo, de VPN: 17 Gbps;

· Deverá suportar, no mínimo, 240.000 novas conexões por segundo;

· Deverá suportar, no mínimo, 3.000.000 de conexões ou sessões simultâneas;

· Deverá suportar os protocolos de roteamento OSPFv2, BGP e RIP;

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

. 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;

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

· Deverá suportar Policy-based routing;

· Deverá possuir fonte de alimentação redundante;

· Deverá possuir, no mínimo, 08 (oito) interfaces de rede 10/100/1000 ou 100/1000/10000 base-T base-T;

· Deverá possuir, no mínimo, 08 (oito) interfaces de rede 10Gbps SFP+; · Deverá suportar, no mínimo, 04 (quatro) interfaces de rede 25Gbps SFP28; · Possuir 1 (uma) interface do tipo console ou similar;

· Possuir 1 (uma) interface de rede dedicada para sincronismo;

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

· O serviço 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;

· Possuir interface dedicada e física para gerenciamento do equipamento fora de banda. Essa interface deve ser um canal de gerenciamento que funcione mesmo quando o dispositivo não responde. Caso o equipamento não possua essa interface física/dedicada, deverá ser composta com outro equipamento de terceiro onde faça essa função. Não sendo permitido qualquer tipo de configuração via software ou uso da interface dedicada de gerenciamento;

· Os equipamentos devem possuir arquitetura modular de interfaces de rede, permitindo a substituição de interfaces por outras com tipo de conexão e velocidades diferentes;

· Deverá possuir, no mínimo, disco Solid State Drive (SSD) com no mínimo 480 GB de capacidade de armazenamento;

· Suportar, no mínimo, a criação de 7 instâncias/contextos virtuais de firewall.

2.3.2. Características específicas mínimas para equipamento para proteção de perímetro do tipo NGFW com SD-WAN – Tipo II

2.3.2.1. Dimensionamento:

· Desempenho requerido, no mínimo, de Next Generation Firewall: 5 Gbps; · Deve possuir capacidade de processamento de, no mínimo, 1.5 (um ponto cinco) Gbps para tráfego stateful inspection TCP completo, sem amostragem, com as funcionalidades de Next Generation firewall, controle de aplicações, IPS e Anti-Malware ativas simultaneamente;

· Desempenho requerido, no mínimo, de VPN: 3.8 Gbps;

· Deverá suportar, no mínimo, 50.000 novas conexões por segundo;

· Deverá suportar, no mínimo, 300.000 conexões ou sessões simultâneas; · Deverá suportar os protocolos de roteamento OSPFv2, BGP e RIP;

· Deverá suportar Policy-based routing;

· Deverá possuir, no mínimo, 8 (oito) interfaces de rede 10/100/1000 base-T; · Deverá possuir, no mínimo, 02 (duas) interfaces de rede 1/10Gbs baseF SFP

sendo que pelo menos uma delas tem ser 10Gbs baseF SFP+;

· Possuir 1 (uma) interface do tipo console ou USB;

· Deverá possuir, no mínimo, disco Solid State Drive (SSD) com no mínimo 256 GB de capacidade de armazenamento.

2.3.3. Características específicas mínimas para equipamento para proteção de perímetro do tipo NGFW com SD-WAN – Tipo III

2.3.3.1. Dimensionamento:

· Desempenho requerido, no mínimo, de Next Generation Firewall: 3.2 Gbps; · Deve possuir capacidade de processamento de, no mínimo, 1.5 (um ponto cinco) Gbps para tráfego stateful inspection TCP completo, sem amostragem, com as funcionalidades de Next Generation firewall, controle de aplicações, IPS e Anti-Malware ativas simultaneamente;

· Desempenho requerido, no mínimo, de VPN: 3.1 Gbps;

· Deverá suportar, no mínimo, 50.000 novas conexões por segundo;

· Deverá suportar, no mínimo, 300.000 conexões ou sessões simultâneas; · Deverá suportar os protocolos de roteamento OSPFv2, BGP e RIP;

· Deverá suportar Policy-based routing;

· Deverá possuir, no mínimo, 8 (oito) interfaces de rede 10/100/1000 base-T; · Deverá possuir, no mínimo, 02 (duas) interfaces de rede 1000 baseF SFP; · Possuir 1 (uma) interface do tipo console ou USB;

· Deverá possuir, no mínimo, disco Solid State Drive (SSD) ou Secure Digital Card (SD) com no mínimo 64 GB de capacidade de armazenamento.

2.3.4. Características específicas mínimas para equipamento para proteção de perímetro do tipo NGFW com SD-WAN – Tipo IV

2.3.4.1. Dimensionamento:

· Desempenho requerido, no mínimo, de Next Generaion Firewall: 1.3 Gbps; · Deve possuir capacidade de processamento de, no mínimo, 660 (seiscentos e secenta) Mbps para tráfego stateful inspection TCP completo, sem amostragem, com as funcionalidades de Next Generation firewall, controle de aplicações, IPS e Anti-Malware ativas simultaneamente.

· Desempenho requerido, no mínimo, de VPN: 2.5 Gbps;

· Deverá suportar, no mínimo, 20.000 novas conexões por segundo;

· Deverá suportar, no mínimo, 175.000 conexões ou sessões simultâneas; · Deverá suportar os protocolos de roteamento OSPFv2, BGP e RIP;

· Deverá suportar Policy-based routing;

· Deverá possuir, no mínimo, 08 (oito) interfaces de rede 10/100/1000 base-T; · Possuir 1 (uma) interface do tipo console ou USB.

· Deverá possuir, no mínimo, disco Solid State Drive (SSD) ou Secure Digital Card (SD) com no mínimo 16 GB de capacidade de armazenamento.

2.3.5. Especificações técnicas mínimas para equipamento para proteção de perímetro do tipo NGFW com SD-WAN – Tipo I, Tipo II , Tipo III e Tipo IV

2.3.5.1. O serviço de proteção de perímetro deve ser composto por appliance de proteção de rede com funcionalidades de proteção de próxima geração;

2.3.5.2. 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;

2.3.5.3. 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;

2.3.5.4. O serviço 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;

2.3.5.5. Realizar upgrade via SCP, SFTP e https via interface WEB;

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

2.3.5.6.1. Suportar VLAN Tags 802.1q;

2.3.5.6.2. Agregação de links 802.3ad;

2.3.5.6.3. Policy based routing ou policy based forwarding;

2.3.5.6.4. Roteamento multicast;

2.3.5.6.5. DHCP Relay e DHCP Server;

2.3.5.6.6. Jumbo Frames.

2.3.5.7. Deve suportar os seguintes tipos de NAT:

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

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

2.3.5.9. Deverá suportar VXLAN;

2.3.5.10. 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;

2.3.5.11. Enviar logs para sistemas de monitoração externos, simultaneamente; 2.3.5.12. 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.Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção;

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

2.3.5.14. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2); 2.3.5.15. Suportar OSPF graceful restart;

2.3.5.15. Autenticação integrada via Kerberos;

2.3.5.16. Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas;

2.3.5.17. O serviço 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);

2.3.5.18. O serviço deve permitir salvar as configurações das politicas para serem aplicadas em horários pré-definidos;

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

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

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

2.3.6. Funcionalidade de filtro de conteúdo WEB exigidas para equipamento para proteção de perímetro do tipo NGFW com SD-WAN – Tipo I, Tipo II , Tipo III e Tipo IV

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

2.3.6.2. Controle de políticas por usuários, grupos de usuários, IPs e redes; 2.3.6.3. Deve de-criptografar tráfego de entrada ou saída em conexões negociadas com TLS 1.2 e TLS 1.3;

2.3.6.4. Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;

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

2.3.6.6. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades: 2.3.6.7. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

2.3.6.8. Reconhecer pelo menos 3.000 (três mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

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

2.3.6.10. Para inspeção SSL, ou HTTPS Inspection, o serviço deve oferecer suporte ao Perfect Forward Secrecy (conjuntos de cifras PFS, ECDHE)

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

2.3.6.12. Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;

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

2.3.6.14. A fim de otimização de tempo operacional dos administrdores, o serviço deverá possuir pelo menos 150 categorias de aplicações WEB pré-definidas pelo fabricante;

2.3.6.15. Paro serviço 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.);

2.3.6.16. Possui mecanismo de controle de aplicação web e URL que possui configuração de bloqueio e liberação da aplicação princial e/ou as suas sub-categorias. Quando o administrador do serviço desejar bloquear apenas as sub-categorias do facebook, como facebook chat, video, game, compartilhamento de arquivos ou outros. Ou seja, não deveser 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. O serviço precisa serbaseada em bloqueio de applicações WEB que a própria base possui, assim a inspeção ocorrerá em camada 7 analisando o payload do pacote.

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

2.3.6.18. Atualizar a base de assinaturas de aplicações automaticamente; 2.3.6.19. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;

2.3.6.20. 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 ou com a instalação do agente no controlador de domínio. Não deve ser preciso instalar agentes nas estações de 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;

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

2.3.6.22. 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;

2.3.6.23. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações; 2.3.6.24. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL: Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora); 2.3.6.25. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

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

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

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

2.3.6.29. 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;

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

2.3.6.31. Suportar a criação de categorias de URLs customizadas;

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

2.3.6.33. Permitir a customização de página de bloqueio;

2.3.6.34. Deve possuir integração com Microsoft Active Directory para identificação de usuários e

2.3.6.35. 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;

2.3.6.36. 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);

2.3.7. Funcionalidades de prevenção de ameaças exigidas para equipamento para proteção de perímetro do tipo NGFW com SD-WAN – Tipo I, Tipo II , Tipo III e Tipo IV

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

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

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

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

2.3.7.5. A fim de não criar indisponibilidade no appliance de segurança, o serviço de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo ou de forma automática;

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

2.3.7.6.1. Análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

2.3.7.7. Detectar e bloquear a origem de portscans;

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

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

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

2.3.7.11. Suportar bloqueio de arquivos por tipo;

2.3.7.12. Identificar e bloquear comunicação com botnets;

2.3.7.13. Deve suportar referência cruzada com CVE;

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

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

2.3.7.14.2. Severidade;

2.3.7.14.3. Tipo de ação executada.

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

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

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

2.3.7.18. 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)

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

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

2.3.7.20. Na própria interface de gerência, a solução de IPS deverá apresentar sumário de todos os equipamentos que estão sendo gerenciados, assim como, qual o tipo de perfil assinalado, de forma individual;

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

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

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

2.3.7.24. O serviço deverá possuir pelo menos dois perfis pré-configurados pelo fabricante que permitam sua utilização assim que o equipamento for configurado;

2.3.7.25. O serviço deve permitir que o administrador possa configurar quais métodos e comandos HTTP são permitidos e quais são bloqueados.

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

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

2.3.7.28. O serviço de IPS deve possuir engine onde irá determinar de forma automática, onde qualquer nova assinatura que for baixada na base local deverá atuar em modo de prevenção ou detecção, assim evitará qualquer tipo de alteração na base de assinatura atual;

2.3.7.29. O Antivírus/Anti-malware deve oferecer suporte à verificação de links dentro de e mails ou ao clicar em links presente em e-mails.

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

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

2.3.7.32. Para melhor administração a solução deve possuir a granularidade na classificação das proteções de IPS através de: severidade, nível de confiança da proteção, impacto da performance, referência de indústria terceira e status de download recente;

2.3.7.33. O serviço deve permitir a criação de White list baseado no MD5 do arquivo;

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

2.3.7.35. Suportar rastreamento de vírus em arquivos pdf;

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

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

2.3.7.38. Em caso de falha no mecanismo de inspeção do Antivírus/Anti-malware, deve ser possível configurar se as conexões serão permitidas ou bloqueada

2.3.7.39. O serviço de Antivírus/Anti-malware deve funcionar de forma independente, ou seja, caso sejam desabilitadas, elas não podem causar a interrupção de outras funcionalidades de segurança como prevenção de ameaças avançadas (zero-day);

2.3.7.40. O serviço de Antivírus/Anti-malware deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS/SMB, de forma a conter Malware se espalhando horizontalmente pela rede;

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

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

2.3.7.43. A solução deverá possuir mecanismo de prevenção de ataques de DNS do tipo DGA (Domain Genaration Algorithm) não sendo aceito soluções que usem apenas mecanismo baseado em assinaturas;

2.3.7.44. Deverá conseguir resolver endereços via DNS, para que conexões com destino a domínios maliciosos, sejam interceptadas pelo Firewall com endereços previamente definidos, para interceptar a comunicação e bloquear o acesso do usuário.

2.3.7.45. O serviço de Anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede.

2.3.7.46. O serviço deve possuir funcionalidade de identificação de bloqueio de trafego malicioso comunicando com C&C (command & Control);

2.3.7.47. O serviço Antivírus/Anti-malware deverá suportar a análise de links no corpo de e mails.

2.3.8. Funcionalidades de controle de qualidade de serviço e SD-WAN exigidas para equipamento para proteção de perímetro do tipo NGFW com SD-WAN – Tipo I, Tipo II , Tipo III e Tipo IV

2.3.8.1. Suportar a criação de políticas de QoS por:

2.3.8.1.1. Endereço de origem, endereço de destino e por porta;

2.3.8.2. O QoS deve possibilitar a definição de classes por:

2.3.8.2.1. Banda garantida, banda máxima e ou fila de prioridade;

2.3.8.3. O serviço 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.

2.3.8.4. Deve permitir limitar a banda (download/upload) usada por aplicações (rate limiting), baseado no IP de origem, usuários e grupos do LDAP/AD;

2.3.8.5. 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.

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

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

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

2.3.8.9. Deve balancear o tráfego de aplicativos em vários links simultaneamente

2.3.8.10. 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

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

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

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

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

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

2.3.8.16. 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.

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

2.3.8.18. Deve ser capaz de criar um túnel otimizado que proteja os aplicativos TCP e UDP contra jitter e perda de pacotes para garantir desempenho de ponta a ponta para áudio, vídeo e tráfego transacional.

2.3.8.19. 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.

2.3.8.20. Capacidade de trabalhar a 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.

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

2.3.8.22. 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).

2.3.8.23. Garantir o desempenho de aplicativos em um cenário de link de transporte duplo quando ambos os links estão degradados simultaneamente

2.3.8.24. Possuir um mecanismo de priorização (QoS) para proteger o tráfego de aplicações prioritárias quando houver congestionamento em pontos remotos

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

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

2.3.8.27. A console de gerenciamento deve informar o status operacional de cada dispositivo que faz parte da rede para operacionalidade

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

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

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

2.3.9. Funcionalidades de VPN exigidas para equipamento para proteção de perímetro do tipo NGFW com SD-WAN – Tipo I, Tipo II , Tipo III e Tipo IV

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

2.3.9.2. Suportar IPSec VPN;

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

; 2.3.9.4. Suportar SSL VPN;

2.3.9.5. A VPN IPSEc deve suportar no minemo:

2.3.9.5.1. SHA-384, AES-XCBC, Diffie-Hellman Group 14, Algoritmo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard), SHA-512 e Autenticação via certificado IKE PKI;

2.3.9.6. A VPN SSL deve suportar:

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

2.3.9.6.2. As funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

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

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

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

2.3.9.6.6. Atribuição de DNS nos clientes remotos de VPN;

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

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

2.3.9.6.9. A solução deve permitir a integração da ferramenta com provedores de identidade, através de SAML, para autenticação dos usuários remotos conectados via VPN;

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

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

2.3.9.6.12. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows 7, Windows 8 e MacOS X;

2.3.9.6.13. Suportar, no mínimo, 100 (cem) clientes VPN SSL simultâneos.

2.3.10. Funcionalidades de proteção contra ameaças avançadas exigidas para equipamento para proteção de perímetro do tipo NGFW com SD-WAN – Tipo I, Tipo II, Tipo III e Tipo IV

2.3.10.1. O serviço deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de Malware não conhecidos e do tipo APT;

2.3.10.2. O serviço deve analisar e bloquear em tempo real e em linha (Inline), as ameaças não conhecidas (zero day). Essa funcionalidade deve ser licenciada em cada appliance de segurança solicitado nesse edital.

2.3.10.3. A solução deverá ser composta por nuvem do próprio fabricante que possui o conceito de sandboxing para prevenção de ataques zero-day.

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

2.3.10.5. A solução deverá operar em modo MTA (Mail Transfer Agent) para proteção de Malware desconhecido de dia zero;

2.3.10.6. Prevenir através do bloqueio efetivo do Malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS) e FTP durante análise completa do arquivo no ambiente sandbox, sem que o mesmo seja entregue parcialmente ao cliente.

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

2.3.10.8. A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows XP, Windows 7, Windows 8.1 e Windows 10, assim como Office 2003, 2010, 2013 e 2016;

2.3.10.9. 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;

2.3.10.10. 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;

2.3.10.11. 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;

2.3.10.12. Toda análise dos arquivos deverá ser realizada em ambiente controlado Sandboxing em nuvem. Não serão aceitas soluções em servidores ou software livre;

2.3.10.13. A funcionalidade de prevenção de ameaças avançadas deve ser habilitada e funcionar de forma independente das outras funcionalidades de segurança;

2.3.10.14. Toda análise deverá ser realizada em nuvem do próprio fabricante, não sendo aceitas soluções que necessitem de módulos e/ou servidores externos para a implementação de máquinas virtuais;

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

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

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

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

2.3.10.19. O relatório das emulações deve conter print screen dos arquivos emulados, assim como todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado;

2.3.10.20. A solução deve possuir engine de inspeção a nivel de CPU para detectar técnicas ROP (Return Of Operation) além de outras técnicas de exploração de vulnerabilidade monitorando o fluxo de CPU;

2.3.10.21. Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;

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

2.3.10.23. Implementar a emulação, detecção e bloqueio de qualquer Malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham Malware desconhecido: pdf, tar, zip, rar, seven- z, exe, rtf, csv, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, doc, docx, dot, docm, dotx, dotm e gz;

2.3.10.24. Toda a análise e bloqueio de Malware 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;

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

2.3.10.26. O serviço deve permitir a criação de Whitelists baseado no MD5 ou SHA 256 do arquivo;

2.3.10.27. No mínimo, o equipamento para proteção de perímetro do tipo NGFW com SD WAN Tipo I deve possuir mecanismo para identificar sites conhecidos e desconhecidos como phishing, analisando em tempo real a URL acessada;

2.3.10.28. O serviço deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas informações em sites classificados como phishing ;

2.3.10.29. O Mecanismo de classificação de anti-phising deve atuar sem a necessidade de instalação de agente na máquina do usuário;

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

2.3.10.31. Número de arquivos emulados;

2.3.10.32. Número de arquivos com Malware.

2.3.10.33. O serviço 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.

2.3.10.34. Caso a solução não possua determinada capacidade, poderá ser integrada com outra solução de mercado, não sendo ela soluções abertas;

2.3.10.35. O serviço deve prover informação, seja por meio de relatório ou log, sobre as seguintes situações:

2.3.10.36. O tamanho máximo do arquivo emulado seja excedido;

2.3.10.37. O tempo máximo de emulação seja excedido.

2.3.11. Funcionalidades de gerenciamento centralizado para equipamento para proteção de perímetro do tipo NGFW com SD-WAN – Tipo I, Tipo II , Tipo III e Tipo IV

2.3.11.1. O serviço de gerência deverá ser separada dos gateways de segurança, que irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas neste documento;

2.3.11.2. Caso o serviço possua licenças relacionadas a capacidade de log indexados e armazenamento, deve ser ofertado a maior capacidade suportada ou ilimitada;

2.3.11.3. Caso o serviço possua módulo de relatórios estendida, deve ser também entregue junto com a solução

2.3.11.4. O serviço deve possuir solução de gerenciamento e administração centralizado, possibilitando o gerenciamento de todos os equipamentos de SD-WAN com proteção de perímetro descritos neste edital;

2.3.11.5. O módulo de gerência deve ser capaz de gerenciar e administrar todas as soluções descritas neste termo;

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

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

2.3.11.8. O gerenciamento do serviço deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS);

2.3.11.9. Todos os logs do serviço devem ser indexados e seu licenciamento deve ser o de maior capacidade.

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

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

2.3.11.12. 3.9. As regras de NAT devem suportar “hit count” para monitorar a quantidade de conexões que deram matches em cada regra;

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

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

2.3.11.15. Suportar validação de regras antes da aplicação;

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

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

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

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

2.3.11.20. Permitir a criação de certificados digitais para autenticação de usuários;

2.3.11.21. O relatório 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 e Sandboxing);

2.3.11.22. O serviço 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.

2.3.11.23. O serviço fornecido deve permitir a integração da ferramenta com provedores de

identidade para autenticação dos administradores da solução via SAML 2.0;

2.3.11.24. O serviço deve possuir logs, correlação de eventos e relatórios de auditoria dos administradores da solução;

2.3.11.25. Permitir criação de relatórios customizados via interface gráfica, sem necessidade de conhecer linguagens de banco de dados;

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

2.3.11.27. Deve ser possível exportar os logs em CSV ou TXT;

2.3.11.28. O serviço deve ser capaz de segmentar a base de regras em uma estrutura em camadas;

2.3.11.29. O serviço deve ser capaz de aplicar proteções relacionadas a ameaças e regras de acesso separadamente;

2.3.11.30. O serviço deve combinar configuração de políticas e análise de logs em um único painel, para evitar erros alcançando maior confiabilidade na alteração de politicas;

2.3.11.31. O visualizador de log deve ter um recurso de pesquisa de texto livre;

2.3.11.32. Deve possibilitar a geração de relatórios de eventos no formato PDF ou HTML;

2.3.11.33. Possibilitar rotação do log;

2.3.11.34. Suportar geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

2.3.11.34.1. Resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda, principais aplicações por taxa de transferência de bytes, principais hosts por número de ameaças identificadas, atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus/Anti-malware), de redes vinculadas a este tráfego;

2.3.11.35. Deve permitir a criação de relatórios personalizados;

2.3.11.36. 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;

2.3.11.37. O serviço 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);

2.3.11.38. Possuir capacidade de integração com soluções de terceiros via API e também suportar configurações através de RestAPI.

2.3.11.39. Deve consolidar logs e relatórios de todos os dispositivos administrados;

2.3.11.40. Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;

2.3.11.41. Deverá possuir mecanismo de Drill-Down para navegação e análise dos logs em tempo real;

2.3.11.42. Nas opções de Drill-Down, deve ser possível identificar o usuário que fez determinado acesso;

2.3.11.43. Gerar alertas de conformidade notificando os usuários sobre o impacto de suas decisões de segurança trazendo as considerações regulatórias na gestão de segurança;

2.3.11.44. Permitir o gerenciamento eficaz das ações e recomendações, facilitando a priorização e programação de itens de ação;

2.3.11.45. Possuir alertas de políticas e as potenciais violações de conformidade;

2.3.11.46. Possuir recomendações de segurança acionáveis e orientações sobre como melhorar a segurança;

2.3.11.47. Gerar relatórios regulamentares com base nas configurações de segurança em tempo real;

2.3.11.48. Permitir que os relatórios possam ser salvos, enviados e impressos;

2.3.11.49. 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;

2.3.11.50. O serviço deve prover, no mínimo, as seguintes funcionalidade para análise avançada dos incidentes:

2.3.11.51. Visualizar quantidade de tráfego utilizado de aplicações e navegação;

2.3.11.52. Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;

2.3.11.53. O serviço de correlação deve possuir mecanismo para detectar login de administradores em horários irregulares;

2.3.11.54. O serviço deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

2.3.11.55. 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;

2.3.11.56. Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory via Radius;

2.3.11.57. Criar certificados digitais para acesso dos usuários VPN;

2.3.11.58. Criar certificados digitais para VPNs Site-to-Site;

2.3.11.59. Caso a solução ofertada para o serviço possua licenciamento relacionado a capacidade de criação de certificados, deve ser contemplado a sua maior capacidade ou ilimitada;

2.3.11.60. Permitir criações de políticas de acesso de usuários autenticada no Active Directory, de forma que reconheça os usuários de forma transparente;

2.3.11.61. 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.

2.3.11.62. 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/Anti-malware e navegação web simultaneamente na mesma query de pesquisa.

2.3.11.63. O relatório das emulações (sandboxing) deve conter print screen dos arquivos emulados, assim como todo detalhamento das atividades executadas em file system, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado;

2.3.11.64. A plataforma de gerência centralizada e monitoração deve possibilitar a procura por IPs e redes, sendo que os resultados mostrem estes IPs e redes nos campos de origem e destino do logs na mesma tela de pesquisa.

2.3.11.65. Possuir mecanismo para que logs antigos sejam removidos automaticamente;

2.3.11.66. Possuir a capacidade de personalização de gráficos como barra, linha e tabela;

2.3.11.67. Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;

2.3.11.68. Deve possuir a capacidade de visualizar na interface gráfica da solução,

informações do sistema como licenças, memória, disco e uso de CPU;

2.3.11.69. O serviço prestado deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real;

2.3.11.70. O serviço deve fornecer conteúdo de correlação pré-definido organizado por categoria;

2.3.11.71. O serviço deve ser capaz de personalizar e criar regras de correlação;

2.3.11.72. O serviço deve fornecer uma interface gráfica para criação das regras citadas no item anterior;

2.3.11.73. O serviço deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências;

ANEXO II - LGPD

DO CUMPRIMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS - LEI N. 13.709/2018

1. É vedado às partes a utilização de todo e qualquer dado pessoal repassado em decorrência da licitação/execução contratual para finalidade distinta daquela do objeto da licitação/contratação, sob pena de responsabilização administrativa, civil e criminal.

2. As partes se comprometem a manter sigilo e confidencialidade de todas as informações – em especial os dados pessoais e os dados pessoais sensíveis – repassados em decorrência da licitação/execução contratual, em consonância com o disposto na Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), sendo vedado o repasse das informações a outras empresas ou pessoas, salvo aquelas decorrentes de obrigações legais ou para viabilizar o cumprimento do instrumento contratual.

3. A LICITANTE/CONTRATADA responderá administrativa e judicialmente, em caso de causar danos patrimoniais, morais, individuais ou coletivos, aos titulares de dados pessoais repassados em decorrência da licitação/execução contratual, por inobservância à Lei Geral de Proteção de Dados.

4. Em atendimento ao disposto na Lei Geral de Proteção de Dados, o STM, para a execução do serviço objeto desta licitação/contrato, tem acesso a dados pessoais dos representantes da LICITANTE/CONTRATADA, tais como número do CPF e do RG, endereços eletrônico e residencial, e cópia do documento de identificação (listar outros, quando cabível).

5. A LICITANTE/CONTRATADA, declara que tem ciência da existência da Lei Geral de Proteção de Dados e se compromete a adequar todos os procedimentos internos ao disposto na legislação com o intuito de proteger os dados pessoais repassados pelo STM.

6. A LICITANTE/CONTRATADA fica obrigada a comunicar ao STM em até 24 (vinte e quatro) horas qualquer incidente de acessos não autorizados aos dados pessoais, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, bem como adotar as providências dispostas no art. 48 da Lei Geral de Proteção de Dados.

7. A LICITANTE/CONTRATADA obriga-se ao dever de proteção, confidencialidade, sigilo de toda informação, dados pessoais e base de dados a que tiver acesso, nos termos da LGPD, suas alterações e regulamentações posteriores, durante o cumprimento do objeto descrito no edital/contrato.

8. A LICITANTE/CONTRATADA não poderá se utilizar de informação, dados pessoais ou base de dados a que tenham acesso, para fins distintos da execução dos serviços especificados no edital/contrato.

9. A LICITANTE/CONTRATADA ficará obrigada a assumir total responsabilidade pelos danos patrimoniais, morais, individuais ou coletivos que venham a ser causados em razão do descumprimento de suas obrigações legais no processo de tratamento dos dados compartilhados pelo CONTRATANTE.

10. Eventuais responsabilidades serão apuradas de acordo com o que dispõe a Seção III, Capítulo VI da LGPD.

ANEXO III- NEPOTISMO

DECLARAÇÃO DE PARENTESCO

IDENTIFICAÇÃO	
01 - Nome	
02 - CPF	**03 - Telefone**
04 -Vínculo com a JMU **( ) Colaborador terceirizado que presta serviços na JMU** **( ) Sócio de empresa que firmou contrato proveniente de Licitação** **( ) Sócio de empresa que firmou contrato proveniente de Dispensa de Licitação** **( ) Sócio de empresa que firmou contrato proveniente de Inexigibilidade de Licitação** **( ) Outro Tipo de Vínculo - Especificar abaixo:**	
05 - Razão Social da Empresa e CNPJ	

Considerando o disposto na Resolução nº 7/05, do Conselho Nacional de Justiça, declaro para os devidos fins que:	
( ) ***não sou*** ***cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de magistrado ou servidor da Justiça Militar da União*****,**	
( ) ***sou*** ***cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de magistrado ou servidor da Justiça Militar da União.***	
07 - Nome do servidor ou magistrado	**08 - Grau de parentesco**
Declaro, ainda, estar ciente de ser o responsável pela atualização das informações aqui prestadas, nos termos da Resolução nº 7/05, do Conselho Nacional de Justiça.	

Brasília, ... de ..... de 2025.

ASSINATURA

(NOME DO RESPONSÁVEL)

(CARGO DO RESPONSÁVEL)

ANEXO IV- DECLARAÇÃO DE NÃO CONDENAÇÃO JUDICIAL POR EXPLORAÇÃO DE TRABALHO INFANTIL

Declaro, em atendimento à vedação do art. 14, VI, da Lei nº 14.133, de 2021, que a empresa _____, inscrita no CNPJ (MF) nº _____, inscrição estadual nº _____, não foi condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista.

Local e data

Assinatura do Representante Legal

Documento assinado eletronicamente por **WILSON MARQUES DE SOUZA FILHO**, **COORDENADOR DE INFRAESTRUTURA DE TECNOLOGIA**, em 20/10/2025, às 15:58 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **MARCIO COELHO MARQUES**, **ANALISTA JUDICIÁRIO - Apoio Especializado - Análise de Sistemas**, em 20/10/2025, às 16:17 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **LUIS GUSTAVO COSTA REIS**, **INTEGRANTE ADMINISTRATIVO**, em 20/10/2025, às 16:27 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **IANNE CARVALHO BARROS**, **DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E TRANSFORMAÇÃO DIGITAL**, em 20/10/2025, às 19:01 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.stm.jus.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **4598601** e o código CRC **13C13633**.

4598601v7