TERMO DE REFERÊNCIA

REGISTRO DE PREÇOS VISANDO FUTURA E EVENTUAL CONTRATAÇÃO DE EMPRESA PARA O FORNECIMENTO DE SOLUÇÃO DE FIREWALL DE PRÓXIMA GERAÇÃO (*NEXT-GENERATION FIREWALL*), INCLUINDO SERVIÇOS DE INSTALAÇÃO, CONFIGURAÇÃO, SUPORTE E GARANTIA

SUMÁRIO

6. DO OBJETO 3
7. DA JUSTIFICATIVA E OBJETIVO DA AQUISIÇÃO 4
8. DA JUSTIFICATIVA PARA UTILIZAÇÃO DO SISTEMA DE REGISTRO DE PREÇOS 8
9. DA FUNDAMENTAÇÃO LEGAL 8
10. DA MODALIDADE LICITATÓRIA 8
11. DO MODO DE DISPUTA 8
12. DOS RECURSOS ORÇAMENTÁRIOS 8
13. DA PARTICIPAÇÃO DE CONSÓRCIOS 8
14. DO CRITÉRIO DE JULGAMENTO DAS PROPOSTAS 9
15. DAS SANÇÕES ADMINISTRATIVAS 9
16. DA PROPOSTA COMERCIAL 11
17. DA QUALIFICAÇÃO TÉCNICA 12
18. DA QUALIFICAÇÃO ECONÔMICO-FINANCEIRA 15
19. DAS INFORMAÇÕES DA FISCALIZAÇÃO 16
20. DOS LOCAIS, PRAZOS E CONDIÇÕES DE ENTREGA 16
21. DO CONTRATO 19
22. DAS SUPRESSÕES OU ACRÉSCIMOS 20
23. DA SUBCONTRATAÇÃO 20
24. DA GARANTIA CONTRATUAL 21
25. DO PAGAMENTO 21
26. DAS OBRIGAÇÕES DA CONTRATADA 24
27. DAS OBRIGAÇÕES DA CONTRATANTE 25
ANEXO I (DO TERMO DE REFERÊNCIA) – ESPECIFICAÇÕES DO OBJETO 28
ANEXO II (DO TERMO DE REFERÊNCIA) – MINUTA DOS TERMOS DO CONTRATO 73

1. DO OBJETO

1.1. Constitui objeto do presente Termo de Referência a **REGISTRO DE PREÇOS VISANDO FUTURA E EVENTUAL CONTRATAÇÃO DE EMPRESA PARA O FORNECIMENTO DE SOLUÇÃO DE FIREWALL DE PRÓXIMA GERAÇÃO (NEXT-GENERATION FIREWALL), INCLUINDO SERVIÇOS DE INSTALAÇÃO, CONFIGURAÇÃO, SUPORTE E GARANTIA**, conforme condições, quantidades e exigências estabelecidas neste instrumento e seus anexos.

ITEM	TIPO	CÓD. MAT. PMV	DESCRIÇÃO RESUMIDA	UNID	QTD
1	HW		NGFW Tipo 1	UN	8
2	HW		NGFW Tipo 2	UN	6
3	HW		NGFW Tipo 3	UN	2
4	HW		NGFW Tipo 4	UN	2
5	SW		Gerenciamento Centralizado de NGFW	UN	2
6	HW		Solução de Armazenamento e Auditoria de Logs	UN	2
7	SE		Treinamento para Solução e Segurança	UN	2
8	SE		Serviço de operação assistida da solução de segurança	Mensal	60
9	SE		Serviço de suporte técnico 8x5	UN	360
10	SE		Instalação e Configuração de NGFW Tipo 1 e 2	UN	14
11	SE		Instalação e Configuração de NGFW Tipo 3 e 4	UN	4
12	SE		Instalação e Configuração de Gerenciamento Centralizado de NGFW	UN	2
13	SE		Instalação e Configuração Solução de Armazenamento e Auditoria de Logs	UN	2
14	HW		Módulo Transceptor SFP-10G-SR	UN	42
15	HW		Módulo Transceptor SFP-10GBASE-T	UN	30

Legendas: "**HW**" – Hardware; "**SW**" – Software; "**SE**" – Serviços.

PERIODICIDADE ESTIMADA DA CONTRATAÇÃO: TRIMESTRAL.

1.2. O processo licitatório se dará por LOTE ÚNICO, visando concentrar em uma única empresa o fornecimento dos produtos e serviços de instalação e configuração do fabricante. Em razão da interdependência dos itens do objeto como um todo, é fundamental, para a garantia da

qualidade do serviço, que sejam fornecidos por um mesmo fornecedor, visando otimizar custos e reduzir o tempo de atendimento em caso de problemas.

1.3. DAS ESPECIFICAÇÕES DO OBJETO

1.3.1. As especificações do objeto estão contidas no **ANEXO I – ESPECIFICAÇÕES DO OBJETO** deste Termo de Referência.

1.4. O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme Decreto Municipal nº 20.934/2022.

2. DA JUSTIFICATIVA E OBJETIVO DA AQUISIÇÃO

2.1. OBJETIVO DA CONTRATAÇÃO

A aquisição de Firewall de Próxima Geração (**NGFW**) e componentes de registro, armazenamento e processamento de LOGs, objetivando aumentar os níveis de segurança cibernética e proteção do ambiente de Tecnologia da Informação e Comunicação (TIC) do Munícipio de Vitória.

2.2. JUSTIFICATIVA

A aquisição de solução de firewall, monitoramento e registro de logs revela-se imprescindível para o robustecimento da segurança cibernética no ambiente da administração pública municipal. Essa medida é vital para assegurar a integridade, a disponibilidade e a confidencialidade dos dados e sistemas que suportam os serviços essenciais de Segurança Pública, Cerco Inteligente, Videomonitoramento e outros. A criticidade desses serviços, por sua vez, exige acesso e interoperabilidade segura com órgãos de segurança municipais, estaduais e federais, incluindo, mas não se limitando a, Polícia Militar, Polícia Civil, SESP, Polícia Federal e Polícia Rodoviária Federal.

Em se tratando de uma solução de segurança cibernética, os tópicos a seguir, apresentam o seu papel na infraestrutura de TIC, bem como detalham cada uma de suas funções.

2.2.1. Firewall – Primeira Linha de Defesa

- **Proteção contra Ameaças Externas:** Um firewall é a primeira linha de defesa contra tentativas de acesso não autorizado, bloqueando tráfego suspeito e protegendo a rede municipal contra os diversos tipos de ataques cibernéticos.
- **Controle de Tráfego:** Um firewall permite o controle e filtragem do tráfego que entra e sai da rede, bloqueando sites e serviços maliciosos e restringindo o acesso a sites que podem comprometer a segurança da rede.
- **Políticas de Segurança Personalizadas:** Com um firewall avançado, a administração pode definir políticas de segurança específicas, restringindo o acesso a informações confidenciais e garantindo que apenas usuários autorizados acessem recursos críticos.

2.2.2. Monitoramento de Rede e Sistema – Visibilidade Contínua e Proativa

- **Identificação de Problemas em Tempo Real:** O monitoramento contínuo permite identificar falhas, sobrecargas e vulnerabilidades na infraestrutura de rede e sistemas municipais, prevenindo indisponibilidades e interrupções de serviços essenciais.
- **Visibilidade Centralizada:** Com uma solução de monitoramento, a equipe de TI pode visualizar todo o ambiente de rede em uma única interface, facilitando a detecção e a resolução de problemas antes que eles afetem os serviços públicos.
- **Prevenção de Incidentes de Segurança:** O monitoramento contínuo também ajuda a identificar comportamentos suspeitos ou atividades que indicam um possível ataque, permitindo medidas proativas antes que incidentes comprometam dados ou operações.

2.2.3. Registro de Logs – Auditoria, Conformidade e Investigação

- **Rastreabilidade e Auditoria:** O registro de logs é essencial para criar uma trilha de auditoria que permite acompanhar quem acessou o quê e quando, viabilizando uma análise detalhada em caso de incidentes.
- **Conformidade com Regulamentações:** A administração pública municipal deve estar em conformidade com regulamentações de segurança e proteção de dados, como a LGPD. A manutenção de logs permite a geração de relatórios para auditorias e comprovações de conformidade.

- **Facilitação de Investigação Forense:** Em caso de incidentes de segurança, os registros de logs fornecem dados essenciais para a análise forense, ajudando a entender como a invasão aconteceu, quais sistemas foram comprometidos e que medidas podem ser tomadas para evitar ataques futuros.

2.3. DOS BENEFÍCIOS DA CONTRATAÇÃO

A nova solução de *NGFW* deve trazer os seguintes resultados de forma resumida:

a) Aumento Significativo do Throughput:

- Capacidade de processamento de dados superior à solução atual.
- Suporte ao crescimento do tráfego de rede sem comprometer o desempenho.

b) Estabilidade no Acesso à VPN:

- Conectividade VPN robusta e confiável.
- Eliminação das falhas frequentes no acesso remoto.

c) Recurso de SD-WAN:

- Otimização da utilização de múltiplos links de comunicação.
- Garantia de alta disponibilidade e melhor desempenho das conexões WAN.

d) Gerenciamento Centralizado:

- Administração unificada de todas as funcionalidades e políticas de segurança.
- Simplificação na aplicação de atualizações e configurações.

e) Certificações de Segurança:

- Comprovação de conformidade com padrões rigorosos de segurança (ex: ICSA, Common Criteria, Netsecopen.org).

f) Inspeção profunda de pacotes (DPI):

- Permite identificar aplicativos e ameaças específicas dentro do tráfego, mesmo quando estão mascarados.

g) Controle baseado em aplicativos:

- Bloqueia ou permite tráfego com base em aplicativos e não apenas em portas e protocolos.

h) Prevenção contra ameaças:

- Integra IDS/IPS (Sistema de Detecção e Prevenção de Intrusões) para mitigar ameaças em tempo real.

i) Suporte a políticas granulares:

- Aplicação de políticas baseadas em usuários, dispositivos, localização ou horário.

j) Integração com segurança avançada:

- Inclui capacidades como sandboxing, inteligência contra ameaças e inspeção SSL/TLS.

k) Importância do Suporte e Garantia

- A nova solução deve ser acompanhada de suporte técnico robusto e garantia abrangente, visando:

l) Sustentação Eficiente do Ambiente:

- Minimização do tempo de inatividade.
- Resolução rápida e eficaz de problemas.

m) Redução do Impacto de Downtime:

- Garantia da continuidade das operações.
- Prevenção de prejuízos financeiros e reputacionais.

n) A aquisição de uma nova solução NGFW é imperativa para:

- Superar os problemas críticos da solução atual.
- Atender às novas demandas tecnológicas e de segurança.
- Assegurar conformidade com normas e requisitos legais.
- Melhorar a segurança da rede municipal.
- Garantir a continuidade e eficiência das operações de TIC.

3. DA JUSTIFICATIVA PARA UTILIZAÇÃO DO SISTEMA DE REGISTRO DE PREÇOS

3.1. O processo licitatório se dará pelo **Sistema de Registro de Preços (SRP)**, posto que tem se mostrado de grande eficiência para a administração, uma vez que permite o crescimento do projeto durante um determinado período, o que proporciona certa flexibilidade na compra, economizando tempo e recursos que seriam dispendidos em um novo processo licitatório.

4. DA FUNDAMENTAÇÃO LEGAL

4.1. A presente aquisição será realizada com fundamento na Lei Federal nº 14.133/2021.

5. DA MODALIDADE LICITATÓRIA

5.1. Trata-se de contratação de serviço comum, a ser contratada mediante licitação, na modalidade **PREGÃO**, em sua forma **ELETRÔNICA**.

6. DO MODO DE DISPUTA

6.1. Em conformidade com o Decreto Municipal nº 20.934/2022, será adotado para o envio de lances o modo de disputa: **ABERTO E FECHADO.**

7. DOS RECURSOS ORÇAMENTÁRIOS

7.1. As despesas decorrentes para a aquisição do objeto desta licitação correrão à conta dos recursos consignados no Orçamento da Prefeitura Municipal de Vitória, para os exercícios alcançados pelo prazo de validade da Ata de Registro de Preços, e será a cargo do Órgão Participante, cujo programa de trabalho e elemento de despesa específica constará na respectiva Nota de Empenho.

8. DA PARTICIPAÇÃO DE CONSÓRCIOS

8.1. Por se tratar de objeto de baixa complexidade, e, considerando que existem no mercado diversas empresas com potencial técnico, profissional e operacional suficiente para

executar o objeto contratado, bem como atender satisfatoriamente às exigências elencadas no Termo de Referência, entende-se que é conveniente a **VEDAÇÃO** de participação de empresas em consórcio no certame em tela e que a participação de empresas em consórcio não ampliaria sua competitividade.

9. DO CRITÉRIO DE JULGAMENTO DAS PROPOSTAS

9.1. Para julgamento das propostas será adotado critério de **MENOR PREÇO.**

10. DAS SANÇÕES ADMINISTRATIVAS

10.1. Os licitantes/adjudicatários/contratados que infringirem as normas constantes deste Termo de Referência ficará(ão) sujeito(s), sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

I. Advertência, nos casos de inexecução parcial que não acarretem prejuízos significativos para a Administração.

II. Multas nos seguintes casos e percentuais:

a) Multa de Mora: Por atraso injustificado na entrega do item contemplado na Autorização de Fornecimento (AF) / Ordem de Serviço (OS) em até 10 (dez) dias: 0,5% (cinco décimos por cento) ao dia sobre o valor da parcela descumprida;

b) Multa Compensatória: Por atraso injustificado na entrega do item contemplado na Autorização de Fornecimento (AF) / Ordem de Serviço (OS) superior a 10 (dez) dias: 10% (dez por cento) sobre o valor total do contrato, com possibilidade de cancelamento da Nota de Empenho Total ou Parcial;

c) Multa Compensatória: Por recusa injustificada do adjudicatário em aceitar ou assinar a Autorização de Fornecimento (AF) / Ordem de Serviço (OS) e/ou Contrato, injustificadamente, uma vez que caracteriza o descumprimento total da obrigação assumida: 15% (quinze por cento) sobre o valor total do contrato;

d) Multa Compensatória: Por entregar em desconformidade, injustificadamente, o objeto contemplado na Autorização de Fornecimento (AF) / Ordem de Serviço (OS): 10% (dez por

cento) sobre o valor total do contrato e possibilidade de cancelamento da Nota de Empenho Total ou Parcial;

e) Multa Compensatória: Por deixar de manter as condições de habilitação durante toda a vigência contrato: 10% (dez por cento) sobre o valor total do contrato, com possibilidade de cancelamento da Nota de Empenho Total ou Parcial;

f) Multa Compensatória: Por inexecução parcial, injustificada, da Autorização de Fornecimento (AF) / Ordem de Serviço (OS): 5% (cinco por cento) sobre o valor total do contrato;

g) Multa Compensatória: Por inexecução total injustificada da Autorização de Fornecimento (AF) / Ordem de Serviço (OS). Caracterizada pela verificação da não entrega do produto/execução do serviço após 30 (trinta) dias: 15% (quinze por cento), sobre o valor total do contrato, com possibilidade de cancelamento da Nota de Empenho Total ou Parcial.

III. Impedimento de licitar e contratar com o Município de Vitória:

a) Dar causa à inexecução parcial da Autorização de Fornecimento (AF) / Ordem de Serviço (OS) e/ou do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo: até 02 (dois) anos;

b) Dar causa à inexecução total da Autorização de Fornecimento (AF) / Ordem de Serviço (OS) e/ou do contrato, caracterizada pela não entrega dos itens após 30 (trinta) dias: até 03 (três) anos;

c) Deixar de entregar a documentação exigida para o certame: até 02 (dois) anos;

d) Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado: até 03 (três) anos;

e) Não celebrar o contrato/instrumento congênere ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta: até 03 (três) anos;

f) Ensejar o retardamento da entrega do objeto da licitação sem motivo justificado, superior a 20 (dez) dias: até 03 (três) anos.

IV. Declaração de inidoneidade para licitar ou contratar com a Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos seguintes casos:

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

b) Fraudar a licitação ou praticar ato fraudulento na execução do contrato;

c) Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

d) Praticar atos ilícitos com vistas a frustrar os objetivos da licitação; e,

e) Praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

11. DA PROPOSTA COMERCIAL

11.1. A Proposta Comercial deverá ser apresentada em moeda nacional utilizando-se até 02 (duas) casas decimais para o valor unitário, desprezando-se as demais, incluindo todos os impostos, seguros, transportes, embalagens, contribuições sociais, bem como quaisquer outros custos relacionados com a entrega do produto, com base nas especificações do objeto.

11.1.1. Ser apresentada com base nas condições e especificações estabelecidas no edital e seus anexos;

11.1.2. Prazo de Validade da Proposta: deverá ter a validade mínima de 60 (sessenta) dias;

11.1.3. Indicar o valor unitário e total por item;

11.1.4. Indicar o valor referente ao valor global para o lote;

11.1.5. Quando houver mais de um item no lote, a empresa arrematante deverá apresentar discriminação do valor unitário e total por item, sendo que o somatório deverá totalizar o valor do referido lote;

11.1.6. Indicar o nome, código do banco, da agência e número da conta corrente;

11.1.7. Indicar a razão social da proponente, endereço completo, telefone, endereço eletrônico (e-mail), bem como: nome, estado civil, profissão, CPF, Carteira de Identidade, domicílio e cargo na empresa, para fins de assinatura do contrato;

11.1.8. Assinatura do representante legal da empresa, devidamente comprovado através da habilitação jurídica, ou Instrumento de Procuração (acompanhado de cópia do documento de identidade do procurador), atribuindo poderes ao outorgado para representar a empresa;

11.1.9. Declarar expressamente que no preço contido na proposta estão inclusos todos os custos, diretos e indiretos, relativos à execução do objeto licitado;

11.2. Não será considerada nenhuma oferta ou vantagem baseada nas propostas dos demais licitantes;

11.3. Serão desclassificadas as propostas que não atenderem ou que forem elaboradas em desacordo com os termos do edital;

11.4. Os preços propostos serão de exclusiva responsabilidade da CONTRATADA, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto;

11.5. A proposta deverá conter oferta firme e precisa, sem alternativas de preços ou qualquer outra condição que induza o julgamento a ter mais de um resultado;

11.6. Outros documentos que devem acompanhar a proposta comercial:

I. MANUAIS, CATÁLOGOS OU FOLHETOS em publicações originais do fabricante, impressos, ou em formato digital, ou em cópias legíveis, indicando marca, modelo e part number do referido equipamento, como forma de comprovação dos requisitos mínimos exigidos nas especificações.

a) Os documentos referenciados deverão ser enviados no formato PDF, de boa resolução, sem senha ou qualquer outro tipo de proteção que impeça a visualização ou a impressão, indicando todas as funcionalidades exigidas neste Termo de Referência e seus anexos.

12. DA QUALIFICAÇÃO TÉCNICA

12.1. Para Qualificação Técnica da Licitante, deverão ser apresentados os seguintes documentos:

I. ATESTADO DE CAPACIDADE TÉCNICA: Comprovação de que a empresa licitante forneceu, sem restrição, solução de segurança da Informação de proteção de tráfego de rede Next Generation Firewall (NGFW), equivalentes a pelo menos 2 (dois) tipos de equipamento NGFW especificados neste Termo de Referência e seus Anexos. A comprovação será feita por meio de apresentação de atestado(s), devidamente assinado(s), carimbado(s), e preferencialmente em papel timbrado da empresa ou órgão tomador do serviço.

a) Para efeito deste Termo de Referência entende-se equipamentos equivalentes aqueles que atendam rigorosamente as especificações definidas para o equipamento em questão;

b) Será admitido o somatório de atestados para fins de atendimento aos critérios de Qualificação Técnica.

- **Justificativa para exigência do ATESTADO DE CAPACIDADE TÉCNICA:**

Confirmação de experiência: O atestado de fornecimento demonstra que a empresa já realizou serviços de implementação similares, anteriormente, comprovando que possui experiência em fornecer Soluções de NGFW. Isso ajuda a reduzir o risco de contratar um fornecedor sem o conhecimento ou infraestrutura adequada.

II. Comprovação de que a proponente é parceira do fabricante da solução ofertada e/ou representante comercial e/ou distribuidor e/ou revendedor autorizado dos equipamentos e serviços de sua fabricação em território nacional. Tal comprovação poderá ser feita por meio de documentação reconhecida, emitida pelo fabricante, ou ainda, por meio de “website” com “url” de acesso público e irrestrito, disponibilizados pelo próprio fabricante, indicando o nome da revenda e seu endereço.

- **Justificativa para exigência do CREDENCIAMENTO:**

A exigência do credenciamento se justifica em razão de que o fornecedor deverá possuir todo o suporte técnico direto com o fabricante do software, evitando possível ausência no fornecimento de suporte ou de atualizações, visando uma prestação dos serviços de excelência à esta municipalidade;

III. A proponente deverá comprovar, em atendimento ao subitem 16.1.14 do Anexo I deste Termo de Referência, de que o fabricante e/ou equipamentos ofertados para os "ITENS 01 ao 04" possuem pelo menos um dos seguintes certificados:

- ✓ ICSA (International Computer Security Association);
- ✓ CC (Common Criteria);
- ✓ Netsecopen.org.

A comprovação se dará por meio de documentação reconhecida, emitida pelos órgãos certificadores, ou ainda, por meio de "website" com "url" de acesso público e irrestrito, disponibilizados pelos órgãos certificadores.

- **Justificativa para exigência de FABRICANTES E SOLUÇÕES CERTIFICADOS:**

Visando assegurar a melhor proposta para a Administração Pública, em atendimento ao Art. 11, I, da Lei nº 14.133/2021, que estabelece a necessidade de critérios objetivos de avaliação, exige-se certificações de segurança reconhecidas internacionalmente para o Fabricante e/ou Equipamento. Essas certificações, obtidas por meio de rigorosa avaliação independente, atestam a conformidade com padrões de segurança da informação, mitigando de forma proativa riscos de ataques cibernéticos complexos, como ransomware e DDoS, e protegendo dados sensíveis de cidadãos e informações estratégicas em escala global. Em consonância com a Política Nacional de Segurança da Informação e Cibernética (PNCiber), que define diretrizes para a proteção de infraestruturas críticas, essa exigência garante a adoção de medidas de segurança adequadas e alinhadas com as melhores práticas do mercado. Adicionalmente, promove a padronização e interoperabilidade com os sistemas existentes na rede de dados da Prefeitura de Vitória, facilitando a integração de novas tecnologias, otimizando a gestão, a manutenção e a segurança da infraestrutura de TIC como um todo.

IV. CERTIFICADO válido de homologação emitido pela Anatel ou por entidade credenciada, para os "ITENS 01 ao 04", em atendimento ao subitem 16.1.15 do Anexo I deste Termo de Referência.

- **Justificativa para exigência de EQUIPAMENTOS HOMOLOGADOS:**

Os equipamentos para telecomunicações, dentre os quais incluem-se os firewalls, precisam de aprovação da Anatel para serem comercializados e utilizados no Brasil. O processo de certificação e homologação tem por objetivo garantir que eles atendam aos requisitos de segurança, qualidade e compatibilidade, protegendo a infraestrutura do país e os usuários contra riscos cibernéticos.

V. DECLARAÇÃO expressa do licitante, preferencialmente em papel timbrado, de que possui no mínimo 01 (um) profissional certificado na solução ofertada, comprovando que o mesmo profissional está treinado e habilitado a realizar serviços de configuração e instalações de seus produtos. A comprovação será realizada na assinatura do contrato, por meio da apresentação de cópia autenticada do contrato social da empresa em caso de sócio, de cópia da carteira de trabalho do profissional em caso de empregado ou contrato de prestação de serviço juntamente com cópia autenticada dos certificados em nome dos profissionais ou declaração emitida pelo fabricante da solução ofertada.

- **Justificativa para exigência dos PROFISSIONAIS CERTIFICADOS:**

Essas certificações são fundamentais para:

- ✓ Realizar instalações escaláveis e seguras;
- ✓ Solucionar problemas técnicos com agilidade;
- ✓ Integrar corretamente os componentes da solução de segurança ofertada;
- ✓ Minimizar riscos operacionais e indisponibilidades, que podem comprometer o perímetro de segurança da rede de dados da Prefeitura de Vitória.

Ressalta-se ainda que tal exigência está fundamentada no inciso III do art. 67 da Lei nº 14.133/2021, que ampara tal exigência, como critério de qualificação técnica.

13. DA QUALIFICAÇÃO ECONÔMICO-FINANCEIRA

13.1. As empresas deverão comprovar Capital Social ou Patrimônio Líquido, no mínimo de 5% (cinco por cento) da soma dos valores ESTIMADOS dos lotes arrematados, conforme

determina a Lei n° 14.133/2021, devendo a comprovação ser feita relativamente à data da apresentação da proposta, na forma da lei.

14. DAS INFORMAÇÕES DA FISCALIZAÇÃO

14.1. A **Gestão** desta aquisição será realizada pelo(a) servidor(a) **RODRIGO GIUBERTI BOITEUX**, matrícula 637755, telefone (27) 3314-3702, e a **Fiscalização** será realizada pelo(a) servidor(a) **FERNANDO PAIVA BEZERRA**, matrícula 603404, telefone (27) 3314-3702 e **JOÃO PAULO MIRANDA COTA**, matrícula 598750, telefone (27) 3317-3702 ou por outro servidor designado, por meio de Ato de Designação do Secretário da Pasta requisitante.

15. DOS LOCAIS, PRAZOS E CONDIÇÕES DE ENTREGA

15.1. A entrega dos itens de hardware da presente licitação dar-se-á no prazo máximo de 60 (sessenta) dias consecutivos, contados do recebimento da Autorização de Fornecimento (AF), em remessa única. No caso de Ordem de Serviços (OS), a CONTRATADA terá um prazo máximo de 30 (trinta) dias corridos para início da prestação dos serviços.

15.2. A(s) entrega(s) deverá(ão) ser realizada(s) no(s) seguinte(s) endereço(s):

15.2.1. Subsecretaria de Tecnologia da Informação: Rua Francisco Rubim, 169, Bento Ferreira, Vitória, ES, CEP 29050-680;

15.3. O horário de recebimento será das **09h às 16h**.

15.4. O local de fornecimento poderá sofrer alteração, a critério da administração, mediante prévia comunicação ao Fornecedor.

15.5. Os locais de instalação serão em qualquer localidade do **Município de Vitória**, sendo a definição feita pelo Fiscal do Contrato;

15.6. O fornecedor deverá atentar para o cumprimento dos prazos, sob pena de aplicação de sanção, em caso de atraso injustificado.

15.7. Os produtos deverão ter garantia mínima conforme especificação de cada item, contado a partir da data de emissão do termo de recebimento definitivo.

15.8. A entrega deverá acompanhar cópia da Autorização de Fornecimento (AF) ou a Nota Fiscal que deverá conter os dados principais do processo de aquisição (nº Processo, nº Licitação, nº AF) a fim de facilitar o recebimento do objeto e agilizar o processo de pagamento.

15.9. O fornecedor fará constar da nota fiscal os valores unitários e respectivos valores totais em conformidade com o constante da correspondente nota de empenho ou contrato, atentando para as inexatidões que poderão decorrer de eventuais arredondamentos.

15.10. O fornecedor deverá garantir a qualidade do objeto, devendo, ainda, quando solicitado, substituir prontamente o que porventura não atenda aos requisitos contratados, sob pena das sanções cabíveis.

15.11. O objeto será recebido provisoriamente, de forma sumária, pelo(a) responsável pelo acompanhamento e fiscalização da contratação, com verificação posterior da conformidade do material com as exigências constantes neste Termo de Referência e na proposta.

15.12. O recebimento provisório deverá ocorrer de forma imediata (no ato da entrega do objeto).

15.13. O objeto poderá ser rejeitado, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de 30 (trinta) dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

15.14. Os bens serão recebidos definitivamente, por servidor ou comissão designada, no prazo de até 15 (quinze) dias, contados do recebimento provisório, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo circunstanciado.

15.15. Na hipótese de a verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo.

15.16. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da CONTRATADA pelos prejuízos resultantes da incorreta execução da contratação.

15.17. Os prazos para os serviços de instalações e configurações conforme relacionados na "Tabela – Itens de Serviços do Lote", considerando sua complexidade, deverão ser realizados, conforme tabela abaixo:

ITENS DE SERVIÇOS DO LOTE		
Item	***Descrição***	***Prazo Máximo***
10	Instalação e Configuração de NGFW Tipo 1 e 2	28 dias
11	Instalação e Configuração de NGFW Tipo 3 e 4	60 dias
12	Instalação e Configuração de Gerenciamento Centralizado de NGFW	34 dias
13	Instalação e Configuração Solução de Armazenamento e Auditoria de Logs	75 dias

Tabela 1: Itens de Serviços do Lote

15.18. Os prazos para os serviços de instalações e configurações conforme relacionados na "Tabela - Itens de Serviços sob demanda do Lote", deverão ser iniciados em até 05 (cinco) dias úteis considerando o recebimento de suas Ordens de Serviço (OS), exclusivamente para os itens:

ITENS DE SERVIÇOS AVULSOS DO LOTE	
Item	***Descrição***
08	Serviço de operação assistida da solução de segurança
09	Serviço de suporte técnico 8x5

Tabela 2: Itens de serviços sob demanda do Lote

15.19. Para a realização do Item "Serviço: Treinamento para Solução e Segurança", este não deverá ultrapassar o prazo máximo de 120 (cento e vinte) dias após o recebimento da primeira Autorizações de Fornecimento (AF).

15.20. Para os Itens: instalação física dos bens e materiais (componentes de hardwares) adquiridos por meio deste certame, ocorrerão após mediante adequação da infraestrutura, tais como: espaço útil em "Rack" no ambiente de datacenter designado, energização e prover meio de passagem dos cabos adquiridos para a conectividade. Estes serviços serão de responsabilidade da equipe técnica designada da CONTRATANTE, e ainda:

15.20.1. Caberá à equipe técnica designada da CONTRATANTE, repassar e realizar todos os demais serviços contendo o repasse de informações e adequações da sua infraestrutura de

conectividade lógica, visando a comportar as novas soluções e/ou componentes (hardwares e softwares) adquiridos através deste certame.

15.21. Para todos os Itens: após o recebimento de sua Autorização de Fornecimento (AF), bem como a assinatura do contrato, em um prazo de até 10 (dez) dias úteis, será realizada uma reunião com a equipe técnica designada, com o(s) profissional(is) designado(s) pela(s) CONTRATADA(S), com intuito de apresentar um resumo dos bens e serviços adquiridos, e ainda, propor um cronograma para a execução dos serviços contratados, onde nesta reunião, deverá apresentar de forma clara e resumida, as fases de execução dos serviços relacionados e contratados a partir deste certame;

16. DO CONTRATO

16.1. O prazo de vigência do contrato será 1825 (mil e oitocentos e vinte e cinco) dias consecutivos, a contar da data de sua assinatura, podendo ser prorrogado conforme o disposto no Art. 107, da Lei 14.133/2021, mediante Termo Aditivo, devidamente autorizada formalmente pela Autoridade Competente.

16.1.1. Poderão ser prorrogados, conforme art. 107 da Lei 14.133/2021, mediante Termo Aditivo, devidamente autorizado formalmente pela Autoridade Competente, somente os itens listados abaixo:

ITEM	TIPO	CÓD. MAT. PMV	DESCRIÇÃO RESUMIDA	UNID	QTD
5	SW		Gerenciamento Centralizado de NGFW	UN	2
7	SE		Treinamento para Solução e Segurança	UN	2
8	SE		Serviço de operação assistida da solução de segurança	Mensal	60
9	SE		Serviço de suporte técnico 8x5	UN	360
12	SE		Instalação e Configuração de Gerenciamento Centralizado de NGFW	UN	2

Legendas: "**SW**" – Software; "**SE**" – Serviços.

16.2. O início da execução deve ocorrer em até 60 (sessenta) dias consecutivos para o fornecimento dos hardwares, contados a partir do recebimento da Ordem de Serviços (OS) / Autorização de Fornecimento (AF).

16.3. O prazo de execução dos serviços será de 1825 (mil e setecentos e sessenta e cinco) dias consecutivos.

17. DAS SUPRESSÕES OU ACRÉSCIMOS

17.1. A Contratada obrigar-se-á a aceitar, nas mesmas condições estabelecidas na Autorização de Fornecimento (AF) / Ordem de Serviços (OS) e/ou Contrato, os acréscimos e supressões que se fizerem necessários, em até 25% (vinte e cinco por cento) do valor inicial atualizado.

18. DA SUBCONTRATAÇÃO

18.1. Devido a existência de serviços de instalação das Soluções, será permitida a subcontratação parcial do objeto, até o limite de 30% (trinta por cento) do valor total contratado.

18.2. É vedada a sub-rogação completa ou da parcela principal da obrigação.

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

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

18.5. Não serão realizados pagamentos diretamente à subcontratadas.

18.6. A subcontratação será formalizada de acordo com o seguinte procedimento:

18.6.1. Submissão, pela CONTRATADA, de pedido fundamentado de que subcontratação, acompanhado de planilha detalhada demonstrando a quantidade e o valor das parcelas que serão subcontratadas;

18.6.2. Autorização prévia, por escrito, da CONTRATANTE para a subcontratação;

18.6.3. Apresentação de cópia do Termo de Subcontratação ou ajuste equivalente celebrado entre a contratada e subcontratada, o qual será juntado aos autos do processo administrativo.

18.7. Somente serão permitidas as subcontratações prévias e regularmente autorizadas pela CONTRATANTE. A subcontratação não formalizada segundo o procedimento previsto neste Termo de Referência, constituirá motivo para a rescisão unilateral do contrato.

18.8. 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 licitação 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.

19. DA GARANTIA CONTRATUAL

19.1. A CONTRATADA fica obrigada a apresentar garantia contratual, em valor correspondente a 5% (cinco por cento) do valor anual do contrato.

20. DO PAGAMENTO

20.1. O pagamento deverá ser solicitado pela CONTRATADA por meio da apresentação no Protocolo Virtual do Município de Vitória (protocolo.vitoria.es.gov.br) da Nota Fiscal ou documento de cobrança equivalente acompanhada dos documentos exigidos no Edital.

20.2. A liquidação da despesa será realizada no prazo de até 10 (dez) dias úteis contados da emissão do Termo de Recebimento Definitivo do objeto.

20.2.1. Após a emissão do Termo de Recebimento Definitivo do objeto, o fiscal da contratação deverá encaminhar imediatamente (no mesmo dia) o processo para o setor responsável pela liquidação da despesa.

20.3. O pagamento será efetuado no prazo de até 07 (sete) dias úteis contados da finalização da liquidação da despesa.

20.3.1. Para atesto do fornecimento serão observados os seguintes aspectos:

a) Critério de Avaliação: FORNECIMENTO, para entrega de bens; EXECUÇÃO, para serviços técnicos;

b) Tipo de pagamento: ÚNICO quando da entrega de bens e POR DEMANDA quando da execução de serviços.

20.4. A(S) NOTA(S) FISCAL(IS) OU DOCUMENTO(S) DE COBRANÇA EQUIVALENTE(S) DEVERÁ(ÃO) SER EMITIDA(S) PARA CADA FONTE DE RECURSO, COM A RAZÃO SOCIAL, CNPJ E ENDEREÇO COMPLETO DO ÓRGÃO REQUISITANTE, CONSTANTES NA AUTORIZAÇÃO DE FORNECIMENTO.

20.5. Na emissão da Nota Fiscal, o fornecedor deverá descrever: o objeto, obrigatoriamente, em conformidade com a descrição contida em sua proposta; o número do processo que originou a contratação; número do contrato; número da Autorização de Fornecimento; e dados bancários, com indicação do banco, agência e conta.

20.6. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.

20.7. A Nota Fiscal ou Documento de cobrança equivalente deverá ser obrigatoriamente acompanhada da documentação prevista no Edital, em conformidade com a Norma de Procedimento de Liquidação de Despesa.

20.8. Constatada a situação de irregularidade em quaisquer das certidões da CONTRATADA, ela será notificada, por escrito, sem prejuízo do pagamento pelo objeto já executado, para,

num prazo de 05 (cinco) dias úteis, regularizar tal situação ou, no mesmo prazo, apresentar defesa, sob pena de rescisão contratual.

20.9. Os pagamentos poderão ser sustados pela Contratante nos seguintes casos:

I. Não cumprimento das obrigações assumidas que possam, de alguma forma, prejudicar o requisitante;

II. Inadimplência de obrigações assumidas pelo fornecedor para com o Município de Vitória, por conta do estabelecido neste Termo de Referência;

III. Erros ou vícios na(s) Nota(s) Fiscal(is)/Fatura(s).

20.10. É vedada a antecipação de pagamentos sem a contraprestação.

20.11. É expressamente vedado a contratada a cobrança ou desconto de duplicatas através de rede bancária ou de terceiros.

20.12. A CONTRATANTE poderá deduzir dos pagamentos importâncias que, a qualquer título, lhe forem devidas pelo fornecedor, em decorrência de inadimplemento das obrigações aqui assumidas, facultando o exercício do contraditório.

20.13. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, o valor devido deverá ser atualizado monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação da seguinte fórmula:

$$\mathbf{VM} = \mathbf{VP} \times \frac{\mathbf{I}}{\mathbf{360}} \times \mathbf{N}$$

Onde:

VM = Valor da multa financeira;

VP = Valor da nota fiscal referente ao mês em atraso;

I = IPCA-IBGE;

N = Número de dias em atraso.

21. DAS OBRIGAÇÕES DA CONTRATADA

21.1. A CONTRATADA deve cumprir todas as obrigações constantes neste Termo de Referência, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

21.1.1. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Termo de Referência e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo, procedência e prazo de garantia ou validade;

21.1.2. A contratada deverá fornecer todos os componentes (Equipamentos, cabos e demais acessórios, softwares e seus licenciamentos) que compõem a Solução ofertada, inclusive no que tange a prestação dos serviços ofertados conforme especificações técnicas e condições exigidas no Termo de Referência deste Edital, cujos custos deverão estar inclusos e inseridos no valor total a ser pago pelo CONTRATANTE;

21.1.3. Substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste Termo de Referência, o objeto com avarias ou defeitos;

21.1.4. Comunicar à Contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

21.1.5. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

21.1.6. Indicar preposto para representá-la durante a execução do contrato;

21.1.7. Assumir a responsabilidade pelos encargos fiscais e comerciais resultantes da adjudicação desta licitação;

21.1.8. Promover a destinação final ambientalmente adequada, sempre que a legislação assim o exigir;

21.1.9. Prestar as informações e os esclarecimentos que venham a ser solicitados pelo Município de Vitória;

21.1.10. A Contratada deve ser responsável por transportar seus funcionários/técnicos/profissionais, ferramentas e equipamentos, para o local de serviço e designados pelo CONTRATANTE;

21.1.11. Responsabilizar-se por quaisquer danos que seus funcionários/técnicos/profissionais causarem ao CONTRATANTE;

21.1.12. Substituir imediatamente qualquer funcionário/técnico/profissional responsável pela execução dos serviços que causar embaraço à boa execução do contrato ou por recomendação da fiscalização ou equipe técnica designada pelo CONTRANTE;

21.1.13. Os funcionários/técnicos/profissionais da empresa licitante contratada, preferencialmente, deverão se apresentar para a realização dos serviços trajando uniforme com logomarca da empresa e portando documento de identificação com foto;

21.1.14. Fornecer cabos UTP's, cabos de conexão direta (DAC) ou transceivers para "Uplinks" bem como cordões de Fibra ótica, nos switches em produção.

22. DAS OBRIGAÇÕES DA CONTRATANTE

22.1. São obrigações da CONTRATANTE:

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

22.1.2. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes deste Termo de Referência e da proposta, para fins de aceitação e recebimento definitivo;

22.1.3. Comunicar à CONTRATADA, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;

22.1.4. Acompanhar e fiscalizar o cumprimento das obrigações da CONTRATADA, através de servidor especialmente designado;

22.1.5. Efetuar o pagamento à CONTRATADA no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos neste Termo de Referência;

22.1.6. Prestar as informações e os esclarecimentos que venham a ser solicitados pelos profissionais ou técnicos da empresa licitante contratada, a ainda, para os profissionais técnicos do(s) fabricante(s) dos componentes que compõem a Solução adquirida;

22.1.7. Tornar disponíveis as instalações e os equipamentos necessários à prestação dos serviços, bem como, os meios necessários para o provimento para instalação e ativação da Solução adquirida, tais como: os “racks” e fornecimento de energia elétrica para alimentação dos componentes envolvidos e necessários do datacenter do CONTRATANTE, e ainda, providenciar “link de dados” e “estrutura lógica” para interconexão junto o ambiente de produção de existente;

22.2. 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.

Vitória, 02 de dezembro de 2025.

Data: 2025.12.02 15:35:27 -03'00'

João Paulo Miranda Cota
Assessor Técnico de TI
Responsável pela elaboração do Termo de Referência
– Fiscal do Contrato –
SEMFA/GAIT

Evandro da Cunha Coelho Sobrinho
Dados: 2025.12.02 15:29:07 -03'00'

Evandro da Cunha Coelho Sobrinho
Assessor Técnico
Responsável pela revisão do Termo de Referência
SEMFA/SUB-TI

Rodrigo Giuberti Boiteux
Dados: 2025.12.02 15:39:45 -03'00'

Rodrigo Giuberti Boiteux
Coordenador de Segurança da Informação
– Gestor do Contrato –
SEMFA/GAIT/CSI

Dados: 2025.12.02 15:38:28 -03'00'

Fernando Paiva Bezerra
Chefe de Equipe de TI
– Fiscal do Contrato –
SEMFA/GAIT/CAR

APROVO OS TERMOS CONSTANTES DO PRESENTE DOCUMENTO E AUTORIZO O PROSSEGUIMENTO DA CONTRATAÇÃO. NA OPORTUNIDADE, DESIGNO O(S) SERVIDOR(ES) MEMBROS DA COMISSÃO TÉCNICA DA SEMFA/SUB-TI COMO RESPONSÁVEIS PARA RESPONDER EVENTUAIS QUESTIONAMENTOS, IMPUGNAÇÕES E RECURSOS ADMINISTRATIVOS, DESDE QUE DE CUNHO TÉCNICO E REALIZAR A ANÁLISE DE DOCUMENTAÇÃO TÉCNICA E AMOSTRAS, CONFORME O CASO.

Vicente de Paulo Braga Secchin
Dados: 2025.12.02 15:31:21 -03'00'

_____

Vicente de Paulo Braga Secchin
Subsecretário de Tecnologia da Informação

ANEXO I (DO TERMO DE REFERÊNCIA) – ESPECIFICAÇÕES DO OBJETO

A tabela seguinte define os itens que compõem a pretendida contratação:

ITEM	TIPO	CÓD. MAT. PMV	DESCRIÇÃO RESUMIDA	QTD	UNID
01	HW		NGFW Tipo 1	8	UN
02	HW		NGFW Tipo 2	6	UN
03	HW		NGFW Tipo 3	2	UN
04	HW		NGFW Tipo 4	2	UN
05	SW		Gerenciamento Centralizado de NGFW	2	UN
06	HW		Solução de Armazenamento e Auditoria de Logs	2	UN
07	SE		Treinamento para Solução e Segurança	2	UN
08	SE		Serviço de operação assistida da solução de segurança	60	Mensal
09	SE		Serviço de suporte técnico 8x5	360	UN
10	SE		Instalação e Configuração de NGFW Tipo 1 e 2	14	UN
11	SE		Instalação e Configuração de NGFW Tipo 3 e 4	4	UN
12	SE		Instalação e Configuração de Gerenciamento Centralizado de NGFW	2	UN
13	SE		Instalação e Configuração Solução de Armazenamento e Auditoria de Logs	2	UN
14	HW		Módulo Transceptor SFP-10G-SR	42	UN
15	HW		Módulo Transceptor SFP-10GBASE-T	30	UN

Legendas: "**HW**" – Hardware; "**SW**" – Software e "**SE**" – Serviços.

1. ITEM 01 - EQUIPAMENTO NGFW TIPO 1

1.1. Características do Hardware (Appliance)

1.1.1. Deve ser capaz de operar nos modos Camada 3 (roteamento), Bridge e Camada 2 (espelhamento de porta) simultaneamente, sem a necessidade de virtualizar o equipamento;

1.1.2. Deve possuir característica de funcionamento de Firewall de última geração (NGFW), não será aceito Firewall de sistema UTM;

1.1.3. Deve ter uma porta dedicada para console e uma porta USB;

1.1.4. Deve ter ao menos 8 (oito) portas Gigabit Ethernet que podem ser portas de interface WAN ou LAN;

1.1.5. Deve ser capaz de utilizar qualquer uma das portas Ethernet fixas como uma porta de Alta Disponibilidade (HA);

1.1.6. Deve suportar o tráfego de 4 (quatro) Gbps de Firewall Throughput;

1.1.7. Deve suportar ao menos 400 (quatrocentos) mil sessões simultâneas;

1.1.8. Deve possuir ao menos 1.6 (um gigabyte e seiscentos megabytes) Gbps de NGFW Throughput;

1.1.9. Deve possuir ao menos 2.5 Gbps (dois gigabytes e quinhentos megabytes) de IPsec VPN Throughput;

1.1.10. Deve possuir ao menos 1.5 (um gigabyte e quinhentos megabytes) Gbps de AV (Antivírus) Throughput;

1.1.11. Deve possuir ao menos 2.6 (dois gigabytes e seiscentos megabytes) Gbps de IPS Throughput;

1.1.12. Deve possuir ao menos 800 (oitocentos) Mbps de Threat Protection Throughput;

1.1.13. Deve possuir ao menos um espaço de armazenamento total de 256 (duzentos e cinquenta e seis) GB SSD ou maior.

2. ITEM 02 - EQUIPAMENTO NGFW TIPO 2

2.1. Características do Hardware (Appliance)

2.1.1. Deve ser capaz de operar nos modos Camada 3 (roteamento), Bridge e Camada 2 (espelhamento de porta) simultaneamente, sem a necessidade de virtualizar o equipamento;

2.1.2. Deve possuir característica de funcionamento de Firewall de última geração (NGFW), não será aceito Firewall de sistema UTM;

2.1.3. Deve ter ao menos uma porta dedicada para console e uma porta USB;

2.1.4. Deve ter ao menos 8 (oito) portas Gigabit Ethernet, 8 (oito) portas SFP e 2 (dois) portas SFP+, que podem ser configuradas como portas de interface WAN ou LAN;

2.1.5. Deve ser capaz de utilizar qualquer uma das portas Ethernet fixas como uma porta de Alta Disponibilidade (HA);

2.1.6. Deve suportar ao menos o tráfego de 20 (vinte) Gbps de Firewall Throughput;

2.1.7. Deve suportar ao menos 7 (sete) milhões de sessões simultâneas;

2.1.8. Deve possuir ao menos 11 (onze) Gbps de NGFW Throughput;

2.1.9. Deve possuir ao menos 11 (onze) Gbps de IPsec VPN Throughput;

2.1.10. Deve possuir ao menos 9 (nove) Gbps de AV (Antivírus) Throughput;

2.1.11. Deve possuir ao menos 14 (quatorze) Gbps de IPS Throughput;

2.1.12. Deve possuir ao menos 6 (seis) Gbps de Threat Protection Throughput;

2.1.13. Deve possuir ao menos um espaço de armazenamento total de 480 (quatrocentos e oitenta) GB SSD ou maior.

3. ITEM 03 - EQUIPAMENTO NGFW TIPO 3

3.1. Características do Hardware (Appliance)

3.1.1. Deve ser capaz de operar nos modos Camada 3 (roteamento), Bridge e Camada 2 (espelhamento de porta) simultaneamente, sem a necessidade de virtualizar o equipamento;

3.1.2. Deve possuir características de funcionamento de Firewall de última geração (NGFW), não será aceito Firewall de sistema UTM;

3.1.3. Deve ter ao menos uma porta dedicada para console e uma porta USB para autoinstalação e configuração;

3.1.4. Deve possuir ao menos 8 (oito) portas Gigabit Ethernet, 8 (oito) portas SFP e 6 (seis) portas SFP+, que podem ser usadas como portas de interface WAN ou LAN;

3.1.5. Deve ser capaz de utilizar qualquer uma das portas Ethernet fixas como uma porta de Alta Disponibilidade (HA);

3.1.6. Deve suportar ao menos o tráfego de 70 (setenta) Gbps de Firewall Throughput;

3.1.7. Deve suportar ao menos 14 (quatorze) milhões de sessões simultâneas;

3.1.8. Deve possuir ao menos 25 (vinte e cinco) Gbps de NGFW Throughput;

3.1.9. Deve possuir ao menos 25 (vinte e cinco) Gbps de IPsec VPN Throughput;

3.1.10. Deve possuir ao menos 25 (vinte e cinco) Gbps de AV (Antivírus) Throughput;

3.1.11. Deve possuir ao menos 35 (trinta e cinco) Gbps de IPS Throughput;

3.1.12. Deve possuir ao menos 15 (quinze) Gbps de Threat Protection Throughput;

3.1.13. Deve possuir ao menos um espaço de armazenamento total de 1.8 TB (um terabytes, oitocentos gigabytes) SSD ou maior.

4. ITEM 04 - EQUIPAMENTO NGFW TIPO 4

4.1. Características do Hardware (Appliance)

4.1.1. Deve ser capaz de operar no modo Camada 3 (roteamento), Bridge e Camada 2 (espelhamento de porta) simultaneamente, sem a necessidade de virtualizar o equipamento;

4.1.2. Deve possuir características de funcionamento de Firewall de última geração (NGFW), não será aceito Firewall de sistema UTM;

4.1.3. Deve ter uma porta dedicada para console e uma porta USB para auto instalação e configuração;

4.1.4. Deve possuir ao menos 8 (oito) portas SFP e 6 (seis) portas SFP+, que podem ser usadas como portas de interface WAN ou LAN;

4.1.5. Deve ser capaz de utilizar qualquer uma das portas Ethernet fixas como uma porta de Alta Disponibilidade (HA);

4.1.6. Deve suportar ao menos o tráfego de 80 (oitenta) Gbps de Firewall Throughput;

4.1.7. Deve suportar ao menos 17 (dezessete) milhões de sessões simultâneas;

4.1.8. Deve possuir ao menos 28 (vinte e oito) Gbps de NGFW Throughput;

4.1.9. Deve possuir ao menos 27 (vinte e sete) Gbps de IPsec VPN Throughput;

4.1.10. Deve possuir ao menos 28 (vinte e oito) Gbps de AV (Antivírus) Throughput;

4.1.11. Deve possuir ao menos 42 (quarenta e dois) Gbps de IPS Throughput;

4.1.12. Deve possuir ao menos 16 (dezesseis) Gbps de Threat Protection Throughput;

4.1.13. Deve possuir ao menos um espaço de armazenamento total de 1.8 TB (um terabytes, oitocentos gigabytes) SSD ou maior.

5. ITEM 05 - GERENCIAMENTO CENTRALIZADO DE NGFW

5.1. Características Gerais

5.1.1. Licenciamento e suporte para 60 (sessenta) meses;

5.1.2. O licenciamento por equipamentos NGFW deve ser da modalidade perpétuo e incluir todos os equipamentos da solução;

5.1.3. A interface de gerenciamento centralizado deve permitir a edição da mesma política de segurança por mais de um usuário administrador de forma simultânea;

5.1.4. Deverá ser instalada em ambiente virtual da CONTRATANTE, devendo estar disponível de forma local (on-site), não sendo permitido soluções de gerenciamento disponíveis em nuvem (cloud). Deve estar disponível para ambientes Nutanix;

5.1.5. Deve permitir o gerenciamento centralizado (interface única de gerência) dos equipamentos a suas configurações de rede, de segurança, gerência de logs, geração de relatórios e sistema de gerência de tráfego WAN;

5.1.6. Deve permitir a definição de um modelo de regras (política de segurança), sobre as quais todas as demais regras ficarão subordinadas, seguindo o conceito de federalização ou hierarquização;

5.1.7. O gerenciamento deve permitir a busca por ativos;

5.1.8. Deve permitir a criação de políticas de acordo com sistema operacional dos usuários;

5.1.9. Deve possuir o agrupamento por tipo;

5.1.10. Deve permitir a visualização da utilização dos links por equipamento;

5.1.11. Deve permitir a visualização das aplicações mais utilizadas em cada link;

5.1.12. Deve possuir a visualização das VPN's, permitindo sua configuração através de ferramenta gráfica para alteração da política;

5.1.13. Caso a solução possua licenças relacionadas a armazenamento, deve ser ofertada a de capacidade ilimitada;

5.1.14. Deve realizar o gerenciamento centralizado das licenças dos equipamentos monitorados;

5.1.15. O gerenciamento deve possuir recurso de comunicação via cliente ou web (GUI), utilizando protocolo seguro (criptografado), encriptação entre equipamento e sistema de gerenciamento;

5.1.16. Caso possua cliente, deve ser compatível e homologado para os sistemas operacionais Windows e Linux;

5.1.17. Deve possuir perfis de acesso a console customizáveis, com permissões granulares, no mínimo com os seguintes perfis: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações, alteração em políticas de acesso;

5.1.18. Deve permitir a localização de regras em que determinado endereço IP, range de IP, sub- rede ou objeto estejam sendo utilizados;

5.1.19. Deve permitir a visualização do número de vezes que uma determinada regra foi usada (hits);

5.1.20. Deve permitir a exportação de logs de auditoria detalhados, no mínimo, informando alterações da configuração realizada com horário das alterações;

5.1.21. Deve possibilitar a coleta de estatísticas do tráfego realizado pelos dispositivos de segurança;

5.1.22. Deve permitir a geração de relatórios, em tempo real, para a visualização de origens e destinos do tráfego gerado pela CONTRATANTE;

5.1.23. Deve possuir visualização sumarizada e permitir gerar relatórios de todas as ameaças (IPS, antivírus, anti-malware) e aplicações trafegadas pelos firewalls gerenciados;

5.1.24. Deve possuir a criação de dashboards customizados, possibilitando a visibilidade do tráfego de aplicações, usuários, ameaças identificadas pelo IPS, antivírus, malwares "Zero Day" detectados em sandbox (quando aplicável) e tráfego bloqueado;

5.1.25. Deve possuir mecanismo "Drill-Down" para visualização, em tempo real, das informações sumárias produzidas pela ferramenta de gerenciamento;

5.1.26. Deve permitir envio de relatórios via e-mail;

5.1.27. Deve possuir a exibição, com histórico e em tempo real (permitindo a filtragem por firewall gerenciado), com atualização automática e contínua, a cada minuto, hora, dia, semana ou mês das seguintes informações:

5.1.28. Deve permitir que os relatórios possam ser exportados em PDF;

5.1.29. Deve possuir a capacidade de gerar alertas.

5.1.30. Em modo cluster, o firewall deve ser atualizado sem interrupções, não havendo interferência no encaminhamento e tratamento das conexões;

5.1.31. Deve exibir a situação do dispositivo e do cluster (geral);

5.1.32. Deve possibilitar filtros para as principais aplicações por classificação (chat, redes sociais, compartilhamento de arquivos) e por volume transferido;

5.1.33. Deve exibir o volume de tráfego transferido nos túneis VPN;

5.1.34. Deve permitir a atualização dos firewalls de forma remota;

5.1.35. Deve permitir a gestão de até 1.000 (mil) dispositivos;

5.1.36. Deve permitir o gerenciamento de todos os equipamentos contratados em uma console única de gerenciamento;

5.1.37. Caso não exista integração e compatibilidade entre os equipamentos ofertados e os existentes, deverá fornecer uma solução para possibilitar a centralização dos logs, informações e configurações, tornando a estrutura única para a CONTRATANTE.

6. ITEM 06 - SOLUÇÃO DE ARMAZENAMENTO E AUDITORIA DE LOGS

6.1. Características de Arquitetura

6.1.1. Deve ser uma solução em formato de appliance virtual e em comercialização pelo fabricante da solução. Não serão aceitas soluções desenvolvidas especificamente para este projeto;

6.1.2. A solução proposta deve suportar armazenamento de até 32 TB;

6.1.3. Deverá suportar grande capacidade de armazenamento, permitindo no mínimo de **3.5TB**, e a possibilidade de expandir até 32TB;

6.1.4. A solução proposta deve suportar no mínimo 30.000 EPS para NAT e 4.000 EPS para Syslog;

6.1.5. Deve ser fornecido Hardware – para fixação em Rack 19'', novo e de primeiro uso – Softwares, Garantia, Suporte e Licenciamento 60 (sessenta) meses, totalmente compatível com a Appliance Virtual do Fabricante seus requisitos e capacidades computacionais, descritas neste Termo de Referência.

6.2. Armazenamento e Monitoramento

6.2.1. Deverá suportar grande capacidade de armazenamento, permitindo no mínimo de 3.5TB, e a possibilidade de expandir até 32TB;

6.2.2. Deverá permitir implantação distribuída e sem impacto ou mudanças no atual ambiente;

6.2.3. Suportar coleta centralizada de logs para ao menos ao quantitativo total de dispositivos de firewall (NGFW) objeto deste Termo de Referência;

6.2.4. Suportar o status de usabilidade do dispositivo, incluindo CPU, memória e armazenamento;

6.2.5. Prover estatísticas de taxa de armazenamento em disco para diferentes tipos de log;

6.2.6. Registrar estatísticas de tendência de recebimento com base no tipo de registro;

6.2.7. Registrar o recebimento de estatísticas de tendências com base em dispositivos;

6.2.8. Deve monitorar o estado de dispositivos que enviam logs;

6.2.9. Deve possuir suporte para monitorar a integridade do disco rígido e o status do RAID;

6.2.10. Deve possuir suporte para personalizar a dashboard de monitoramento.

6.3. Armazenamento e Consultas de Logs

6.3.1. Suportar consultas personalizadas ou filtro de condições para: log de eventos, log de rede, log de configuração, log IPS, log de ameaças, log de segurança, log de sessão, log PBR, logs NAT (incluindo NAT444), log de URL, log de e-mail, e outros;

6.3.2. Suportar log de sessão IPv6, log NAT, log PBR, log SLB;

6.3.3. Suportar coleta e consulta de logs de terceiros;

6.3.4. Deve possibilitar diferenciar o nível de log por cores;

6.3.5. Suporte a Logs do Windows;

6.3.6. Permitir a consulta de combinação de logs por múltiplas condições;

6.3.7. Suportar pesquisa de texto completo do campo URL;

6.3.8. Deverá possuir suporte a consultas de tarefas em segundo plano e notificações por e-mail;

6.3.9. Suportar a manutenção de condições de consulta salvas;

6.3.10. Deverá possuir suporte a consultas distribuídas;

6.3.11. Deverá possuir suporte a registros de segurança de dados;

6.3.12. Suportar os logs IPv6;

6.3.13. Deverá possuir suporte para análise, armazenamento e exibição dos novos logs de firewall;

6.3.14. Deverá possuir suporte para upload de modelo de análise de syslog;

6.4. Relatórios Estatísticos

6.4.1. O conteúdo estatístico de relatório deverá incluir:

6.4.1.1. Recursos do sistema;

6.4.1.2. Classificação de quantidade de log de dispositivos;

6.4.1.3. Classificação de ocupação de espaço de log de dispositivos;

6.4.1.4. Classificação de quantidade de log;

6.4.1.5. Classificação de espaço total de log;

6.4.1.6. Classificação de quantidade de log com base no IP de origem;

6.4.1.7. Classificação de quantidade de log com base no IP de destino;

6.4.1.8. Classificação de tendências de recebimento de log;

6.4.1.9. Quantidade de ameaças/ataques;

6.4.1.10. Registro de sessão;

6.4.1.11. Acesso ao APP;

6.4.1.12. Classificação de acesso à URL, entre outros.

6.4.2. Suportar relatórios periódicos por dia, semana, mês, trimestre.

6.4.3. Os relatórios deverão ser gerados e classificados por minutos, horas ou dias.;

6.4.4. Deve permitir a geração de relatórios em formados HTMP, PDF ou WORD;

6.4.5. Deve permitir o envio de relatórios podem ser enviados por e-mail;

6.4.6. Deve possuir relatórios personalizados e relatórios predefinidos;

6.4.7. Deve possuir relatório de suporte de estatísticas de tráfego;

6.5. Administração do Sistema

6.5.1. Suportar limpeza automática de disco com base em limites personalizados de armazenamento;

6.5.2. Suportar o cadastro de host confiável, permitindo o acesso limitado apenas através desses hosts cadastrados;

6.5.3. Suportar horário de verão automático;

6.5.4. Suportar acesso HTTP e HTTPS;

6.5.5. Suportar transmissão de logs via SSL;

6.5.6. Suportar função de gerenciamento de senha para configurar o comprimento mínimo e a complexidade da senha, o número máximo de falhas de login e o tempo de bloqueio após exceder o número máximo de falhas de login;

6.5.7. Deve suportar NFS para armazenamento;

6.5.8. Suportar modificação de nome de usuário do administrador padrão.

6.6. Backup e Gestão de Logs

6.6.1. Deverá suportar backup de logs para ambiente externo através de FTP e SFTP;

6.6.2. Deve suportar o encaminhamento de logs para servidor externo;

6.6.3. Deverá permitir a importação de registros de logs;

6.6.4. Deve permitir a limpeza de registros de logs;

6.6.5. Suportar ativação da versão de teste online/offline.

7. ITEM 07 - TREINAMENTO PARA SOLUÇÃO DE SEGURANÇA

7.1. A CONTRATADA deverá prestar serviços de treinamento oficial para até 6 (seis) servidores da SUBTI devidamente indicados, com as características descritas a seguir:

7.1.1. Turma deve ser composta com no máximo 6 (seis) participantes;

7.1.2. Turma com carga horária mínima de 40 (quarenta) horas;

7.1.3. As datas de aplicação dos treinamentos deverão ser fixadas, em comum acordo com a CONTRATANTE e CONTRATADA;

7.1.4. O conteúdo do treinamento deverá abranger:

7.1.4.1. Apresentação da arquitetura da solução;

7.1.4.2. Visão geral de funcionamento da solução;

7.1.4.3. Configurações e Parâmetros da Solução.

7.1.5. O material didático deverá ser repassado de forma impressa e/ou por meio de mídia digital para os participantes;

7.1.6. Os instrutores deverão possuir certificação comprovada do fabricante;

7.1.7. O treinamento poderá ocorrer no formato remoto ou presencial, em comum acordo entre CONTRATANTE e a CONTRATADA, considerando o seguinte:

7.1.7.1. Em caso de treinamento remoto:

7.1.7.1.1. A CONTRATANTE ficará responsável pela infraestrutura computacional de uso individual dos participantes (notebooks, webcams, microfones e headsets) e interconectividade necessária (internet Wi-Fi ou cabeada);

7.1.7.2. Em caso de treinamento presencial:

7.1.7.2.1. A CONTRATANTE ficará responsável pelo equipamento de uso individual dos participantes (notebooks, webcams, microfones e headsets);

7.1.7.2.2. A CONTRATADA ficará responsável por montar o local para realização do treinamento, isto é, todo o espaço necessário assim como toda infraestrutura computacional e interconectividade necessária.

7.1.8. Caberá à empresa CONTRATADA instalar a plataforma e demais softwares que compõem a solução ou possibilitar o acesso para o treinamento;

7.1.9. Todas as despesas relativas à execução do treinamento serão de exclusiva responsabilidade da empresa CONTRATADA, incluindo os gastos com instrutores, alimentação, estadia e o seu deslocamento;

7.1.10. Para fins de comprovação da execução dos Serviços de Treinamento, a contratada deverá entregar:

7.1.10.1. Lista de presença dos participantes do treinamento;

7.1.10.2. Ficha de avaliação do treinamento preenchida e assinada pelos participantes, considerando:

7.1.10.2.1. Nome do Treinamento;

7.1.10.2.2. Nome do Participante;

7.1.10.2.3. Data do Treinamento;

7.1.10.2.4. Nome do Instrutor;

7.1.10.2.5. Bem como:

Ficha de Avaliação	Ruim	Regular	Bom	Ótimo
Conteúdo do Curso foi adequado?				
A utilização dos recursos didáticos foi adequada?				
O ambiente digital para o treinamento foi adequado?				
O material didático foi adequado?				
O tempo de treinamento foi suficiente?				
O Instrutor apresentou possuir domínio do conteúdo?				
Avaliação geral do Treinamento				

Tabela 3: Ficha de avaliação

7.1.11. Certificado de execução do treinamento nominal para cada participante ao término do treinamento.

8. ITEM 08 - SERVIÇO DE OPERAÇÃO ASSISTIDA DA SOLUÇÃO DE SEGURANÇA

8.1. Serviço onde a CONTRATADA, por meio de especialistas, com conhecimento aprofundado sobre a solução instalada e uma abordagem proativa para simplificar e otimizar as implantações e operações relacionadas, visa manter a estrutura da Solução de Segurança da Informação bem gerenciada, saudável e com bom desempenho;

8.2. Cada unidade deste item deve considerar 1(hum) mês de operação remota/presencial do técnico, na região, durante o horário comercial local e suportado por notificações e gerenciamento de escalonamento 24 horas por dia, 7 dias por semana;

8.3. As atividades contratadas desse item não possuem conflito com as atividades de manutenção, substituição de peças e suporte do fabricante dos equipamentos.

8.4. Características Gerais:

8.4.1. Eliminar a exposição através do aconselhamento proativo sobre as melhores práticas de segurança e gerenciamento de riscos conhecidos;

8.4.2. Prevenir riscos e melhorar continuamente os resultados associados às operações relacionadas a solução;

8.4.3. Acompanhamento para a verificação da “Status/Saúde”, assim como, a revisão de configuração junto a solução de software, incluindo ainda, relatórios ou procedimentos contendo indicações com base nas orientações recomendadas pelo seu fabricante, e ainda, conforme as necessidades indicadas pela equipe técnica designada;

8.4.4. Acompanhamento para a verificação e/ou revisão de configurações junto as funcionalidades e/ ou recursos, incluindo no auxílio à procedimentos contendo indicações com base nas orientações recomendadas e sugeridas pelo(s) fabricante(s), ou ainda, conforme as necessidades indicadas pela equipe técnica designada;

8.4.5. Verificação e/ou revisão de configurações das rotinas ou políticas de replicação, ou de recuperação de desastres, quando implementados, incluindo no auxílio com sugestões e orientações recomendadas pelo fabricante, ou ainda, conforme as necessidades indicadas pela equipe técnica designada;

8.4.6. Preparar e auxiliar a equipe do CONTRATANTE para assumir novos projetos com planejamento e treinamento conjunto.

8.5. Acionar o Fabricante para atividades junto ao CONTRATANTE:

8.5.1. Ponto focal primário e proativo no fabricante para tratar de assuntos técnicos e de suporte especializado;

8.5.2. Coordenar reuniões de especialistas em produtos, engenharia, suporte e serviços;

8.5.3. Coordenar com o CONTRATANTE questões técnicas e críticas para o negócio;

8.5.4. Priorizar novos recursos solicitados pelo CONTRATANTE;

8.5.5. Coordenar temas relacionados à vários produtos do fabricante e escalonamentos quando eles ocorrerem.

8.6. Gestão de Risco Operacional:

8.6.1. Realizar verificações de integridade abrangentes e apresentar recomendações para abordar as descobertas;

8.6.2. Conduzir e coordenar o gerenciamento, escalonamento e resolução de problemas;

8.6.3. Melhorar a utilização da capacidade - analisar, otimizar e recomendar soluções;

8.6.4. Otimizar o gerenciamento de serviços e a otimização do uso de licenças;

8.6.5. Revisar todo o software e firmware e fornecer recomendações para padronização e economia.

8.7. Análise e relatórios:

8.7.1. Analisar relatórios de serviço personalizados: tempo de atividade, utilização e confiabilidade de software e hardware;

8.7.2. Análise de capacidade e utilização;

8.7.3. Auditorias de desempenho e saúde, bem como relatórios;

8.7.4. Análise de eventos e relatórios sobre casos críticos, incluindo causa raiz.

8.8. Planejamento de negócios e suporte:

8.8.1. Desenvolver plano e recomendar estratégia para escalar, maximizando o Retorno sobre o investimento;

8.8.2. Definir métricas de sucesso para o negócio;

8.8.3. Planejar e se preparar para eventos significativos ou lançamentos de grandes projetos;

8.8.4. Revisar o ciclo de vida de software e hardware.

8.9. Educação e melhores práticas:

8.9.1. Avaliação de aprendizagem da equipe técnica do CONTRATANTE;

8.9.2. Facilitar a capacitação de produtos e tecnologias;

8.9.3. Compartilhar melhores práticas por meio de manuais, artigos técnicos e documentos de especificações para o ambiente do CONTRATANTE;

8.9.4. Facilitar apresentações do portifólio de produtos com especialistas do fabricante.

8.10. Resultados apresentados:

8.10.1. Mensalmente a CONTRATADA deve apresentar relatórios sobre o Ambiente computacional, constando:

8.10.1.1. Nível de disponibilidade do Ambiente;

8.10.1.2. Nível de resiliência do ambiente;

8.10.1.3. Alertas e falhas;

8.10.1.4. Atividades desenvolvidas no mês referido;

8.10.1.5. Procedimentos ou mudanças futuras (quando aplicável) que devem ser previamente agendados.

8.11. Nas situações de não cumprimento das atividades estabelecidas nesse item, a aplicação de penalidades previstas, conforme tabela abaixo:

CONDIÇÕES	MEDIDAS CORRETIVAS
Não apresentação dos relatórios mensais.	Advertência
Ausência de atividades conforme descritas no item.	Sanções previstas em contrato.

Tabela 4: Penalidades operação assistida

9. ITEM 09 - SERVIÇO DE SUPORTE TÉCNICO 8X5

9.1. Trata-se de Serviço de suporte técnico, na prestação de atendimento remoto/presencial quando impossibilidade justificada de acesso a Plataforma, para os produtos e soluções em produção, sendo prestados apenas, na modalidade “8x5” (oito horas por dia, pelos cinco dias da semana), e ainda, em dia e hora útil (segunda a sexta-feira, de 08h00 às 18h00, exceto feriados).

9.2. São atividades relativas a incidentes e sua tratativa, sendo: indisponibilidade, baixo desempenho, erros, falhas de hardware ou software, falhas de operação ou configurações incorretas, que venham a ocorrer no ambiente de NGFW.

9.3. Cada chamado aberto e contratado através deste item de serviço, será considerado até 08 horas úteis de prestação de serviço, sendo esse, do início do atendimento até a sua conclusão.

9.4. A medição é realizada por chamado concluído.

9.5. Cada unidade representa um chamado.

9.6. A abertura de chamados, deve ser previamente condicionada ao escopo do serviço solicitado pela CONTRATANTE, sendo analisado a abertura de outros chamados para atendimento completo ao escopo proposto, através da contratação de mais itens desse serviço, sob comum acordo entre a CONTRATANTE e a CONTRATADA.

9.7. Essas atividades serão solicitadas pela CONTRATANTE ou abertas automaticamente por meio de interoperabilidade da Solução (quando solicitado pela CONTRATANTE), no Sistema da Central de Atendimento da CONTRATADA. Devendo ser executadas por profissionais especializados na Solução de Segurança da Informação e acompanhamento da equipe designada.

9.8. Esse serviço possui as seguintes características:

9.8.1. A CONTRATADA deverá disponibilizar uma “Central de Atendimento” para os serviços de registro e abertura de chamados, a qual, também deverá permitir que a equipe técnica designada, ou por terceiros indicados pelo CONTRATANTE, possam acompanhar esses

chamados de forma centralizada, seja através de “Teleatendimento”, “Endereço Eletrônico (E-mail)” e “Sistema Web”, os quais, esses chamados registrados e abertos, deverão ocorrer, nas situações de defeitos e/ou falhas relacionados exclusivamente aos produtos e soluções em produção, incluindo ainda:

9.8.1.1. A CONTRATADA, ainda deverá iniciar o atendimento de “Serviço de Suporte Técnico Remoto”, através do seu profissional designado, conforme os níveis e prazos relacionados na “Tabela - Nível de Classificação do Incidente / Problema vs Tempo de Atendimento” abaixo:

CLASSIFICAÇÃO (NÍVEL)	CARACTERÍSTICAS (INCIDENTES / PROBLEMAS)	TEMPO DE ATENDIMENTO
Prioridade I (Crítica)	As operações do sistema pararam junto à solução em produção. O ambiente está passando por uma interrupção de dados com um problema crítico e impacto nas suas atividades e dados.	Até 02 horas úteis para início do atendimento
Prioridade II (Alta)	Impacto real ou parcial nas operações do sistema junto à solução em produção, ou, ainda, interrupção parcial das atividades ou dados. O ambiente está apresentando falha de componentes, ou mudanças significativas de desempenho do mesmo.	Até 04 horas úteis para início do atendimento
Prioridade III (Normal)	Impacto real ou parcial no desempenho do sistema junto à solução em produção. O ambiente está apresentando alguma anormalidade no seu desempenho, ou mesmo, alguém comportamento anormal em sua produção.	Até 08 horas úteis para início do atendimento
Prioridade IV (Baixa)	Ações comuns de baixo impacto, tais como: redefinições de senha, ou consultas de processos ou solicitações de documentações, ou ainda, ou solicitações de atualização de softwares e firmwares, junto à solução em produção.	Até 24 horas úteis para início do atendimento

Tabela 5: Nível de Classificação do Incidente / Problema vs Tempo de Atendimento

9.8.2. A CONTRATADA, deverá fornecer atestado comprovando a existência junto a sua equipe técnica, no mínimo 01 (um) ou mais profissionais designados capacitados e detentores de “Certificados / Certificações” emitidos pelo fabricante da Solução, ou seja, para solução de software que compõem os equipamentos em produção, sendo permitido:

9.8.2.1. A apresentação do mesmo "Certificado" ou "Certificação", e demais comprovações solicitadas conforme as condições solicitadas no Termo de Referência deste Edital.

9.8.3. A CONTRATADA será eximida da aplicação das sanções administrativas para os respectivos chamados registrados e abertos, em que sejam descumpridos os prazos de atendimento e respostas, desde que comprovadas as seguintes situações:

9.8.3.1. Quando constatado que o problema está relacionado a um "bug" no produto ou solução, o qual, o fabricante não possua correção imediata para tal, sendo este fato declarado pelo próprio;

9.8.3.2. Quando através de seu profissional designado, forem tomadas todas as medidas possíveis visando providenciar solução de contorno;

9.8.3.3. Quando através de se profissional designado, for diagnosticado problemas relacionados ao ambiente de datacenter ou mesmo de problemas de infraestrutura local, ocasionados por equipamentos ou soluções que não fazem parte do Objeto dessa licitação;

9.8.3.4. Não será responsável por substituições de quaisquer peças, componentes ou outros materiais que apresentarem defeitos de fabricação, mesmo que, substituídos por outros originais, os quais, não possuem "Garantia e/ou Suporte" devidamente ativos e provisionados juntos aos bens e materiais que compõem à solução em produção.

9.8.4. A equipe técnica designada, ou por terceiros indicados pelo CONTRATANTE, deverá ser a responsável em prover acesso remoto exclusivamente, para o profissional designado ou para os analistas designados pelos fabricantes dos produtos e soluções que compõem a solução em produção, para realização dos serviços de suporte e/ou assistência técnica junto aos mesmos, quando solicitados, esse acesso deverá ser disponibilizado durante toda a vigência do contrato do Objeto deste Edital;

9.8.5. O método de trabalho para este item de serviço, será baseado no conceito de "Delegação de Responsabilidade" atribuída diretamente e exclusivamente pela equipe técnica designada, inclusive quanto a sua solicitação e aprovação junto "Termo de Aceite / Relatório Técnico", o qual, posteriormente deverá ser submetido para autorização de pagamento pelo

"Gestor de Contrato" designado pelo CONTRATANTE. Portanto a gestão qualitativa dos resultados obtidos e sua aprovação, será por meio da execução dos serviços dentro dos prazos e níveis indicados, e ainda, pelo reestabelecimento do funcionamento dos produtos e soluções que compõem a solução em produção, indicados no processo de registro e abertura do seu chamado relacionado;

9.8.6. Cabendo à CONTRATADA, nas situações de não cumprimento dos prazos e níveis previamente estabelecidos, à aplicação de penalidades previstas pelo CONTRATANTE junto a unidade deste item contratado, conforme tabela abaixo:

PERCENTUAL DOS CHAMADOS EM ATRASO APÓS A ABERTURA	***TEMPO DE ATRASO PARA ATENDIMENTO***	***MEDIDAS CORRETIVAS***
Maior que 20%	<= 08 horas úteis	Nenhuma
	> 08 e <=24 horas úteis	Advertência
	> 48 horas úteis	Sanções previstas em contrato

Tabela 6: SLA x Penalidades

10. ITEM 10 - INSTALAÇÃO E CONFIGURAÇÃO DE NGFW TIPO 1 e 2

10.1. Todas as fases de planejamento, instalação e configuração deverão ser realizadas com a presença de técnicos da CONTRATADA, que deverão possuir capacidade técnica necessária à execução do serviço;

10.2. Os trabalhos deverão ser realizados dentro do horário comercial, das 08:00 às 18:00, salvo casos em que necessite parada no ambiente que demande janelas de manutenção. Neste último caso, deve ser negociado os horários com antecedência;

10.3. Deve ser realizado previamente ao início dos trabalhos uma análise da topologia e arquitetura da rede, considerando os demais equipamentos de segurança do ambiente da CONTRATANTE;

10.4. Toda a instalação e configurações a serem realizadas devem ser de acordo com as melhores práticas do fabricante;

10.5. Este serviço deverá incluir:

10.5.1. Configuração e Parametrização lógica da solução contratada;

10.5.2. Projeto de configuração, contemplando todas as informações de ativação;

10.5.3. Após a instalação dos ativos físicos, atividades de integrações e customizações poderão ser realizadas de forma física e remota.

10.6. Criação de Template de configuração;

10.7. Deverá ser ministrado um treinamento do tipo "Repasse de conhecimento" para operação da Solução com duração de até 08 (oito) horas;

10.8. Deverá ser entregue documentação detalhada ao final da realização dos trabalhos contendo o passo-a-passo de toda instalação e configuração dos equipamentos envolvidos no projeto;

10.9. A instalação deverá ser dividida nas seguintes etapas:

10.9.1. Análise de Requisitos

10.9.1.1. Nesta fase a CONTRATADA terá até 7 (sete) dias para inventariar e fornecer todos os requisitos projeto, bem como os recursos necessários para a execução. É importante que a CONTRATADA use de comunicações através de reuniões com a equipe técnica que executará o projeto;

10.9.1.2. Nesta fase deverá haver um pré-kickoff de projeto, com o objetivo de apresentar as equipes envolvidas no projeto e esclarecer dúvidas sobre escopo dos serviços previsto no Termo de Referência, definir papéis e responsabilidades e esclarecer qualquer outro ponto relevante sobre a execução e medição do projeto.

10.9.2. Planejamento

10.9.2.1. Esta fase deverá ser realizada em até 7 (sete) dias, contados da data de finalização da última fase, e deverá ser composta de:

10.9.2.2. Apresentação do Termo de Abertura do Projeto com matriz de responsabilidades, riscos envolvidos;

10.9.2.3. Apresentação do cronograma analítico do projeto com os responsáveis por executar cada atividade, estimativa de datas e períodos de execução, etapas e atividades;

10.9.2.4. Apresentação do plano de integrações que serão realizadas entre as plataformas do fabricante e os demais ativos da CONTRATANTE;

10.9.2.5. A CONTRATANTE designará um responsável técnico para ser o facilitador entre as áreas técnicas da CONTRATANTE, que providenciará os acessos, integrações e ações de preparação necessárias de serem realizadas nos ativos de sustentação da CONTRATANTE, para integrar as tecnologias que serão monitoradas.

10.9.3. Execução

10.9.3.1. Esta fase deverá ser realizada em até 7 (sete) dias, contados da data de finalização da última fase, e deverá ser composta de:

10.9.3.1.1. Instalação dos Appliances que compõem a solução;

10.9.3.1.2. Configuração dos ativos e consoles que compõem a solução;

10.9.3.1.3. Filtragem dos logs de eventos de segurança;

10.9.3.1.4. Confecção de dashboards ou ativação de dashboards padrão;

10.9.3.1.5. Confecção de relatórios ou ativação de relatórios padrão;

10.9.3.1.6. Instalação de agentes de segurança necessários;

10.9.3.1.7. Criação dos casos de uso conforme descritos no termo de referência.

10.9.4. Encerramento

10.9.4.1. Esta fase deverá ser realizada em até 7 (sete) dias:

10.9.4.1.1. Revisão de todos os pontos da execução;

10.9.4.1.2. Confirmação das integrações realizadas conforme previsto no cronograma do projeto e escopo do edital;

10.9.4.1.3. Emissão do relatório de medição e termo de encerramento do projeto.

11. ITEM 11 - INSTALAÇÃO E CONFIGURAÇÃO DE NGFW TIPO 3 e 4

11.10. Todas as fases de planejamento, instalação e configuração deverão ser realizadas com a presença de técnicos da CONTRATADA, que deverão possuir capacidade técnica necessária à execução do serviço;

11.11. Os trabalhos deverão ser realizados dentro do horário comercial, das 08:00 às 18:00, salvo casos em que necessite parada no ambiente que demande janelas de manutenção. Neste último caso, deve ser negociado os horários com antecedência;

11.12. Deve ser realizado previamente ao início dos trabalhos uma análise da topologia e arquitetura da rede, considerando os demais equipamentos de segurança do ambiente da CONTRATANTE;

11.13. Toda a instalação e configurações a serem realizadas devem ser de acordo com as melhores práticas do fabricante;

11.14. Este serviço deverá incluir:

11.14.1. Configuração e Parametrização lógica da solução contratada;

11.14.2. Projeto de configuração, contemplando todas as informações de ativação;

11.14.3. Após a instalação dos ativos físicos, atividades de integrações e customizações poderão ser realizadas de forma física e remota.

11.15. Criação de Template de configuração;

11.16. Deverá ser ministrado um treinamento do tipo “Repasse de conhecimento” para operação da Solução com duração de até 08 (oito) horas;

11.17. Deverá ser entregue documentação detalhada ao final da realização dos trabalhos contendo o passo-a-passo de toda instalação e configuração dos equipamentos envolvidos no projeto;

11.18. A instalação deverá ser dividida nas seguintes etapas:

11.18.1. **Análise de Requisitos**

11.18.1.1. Nesta fase a CONTRATADA terá até 7 (sete) dias para inventariar e fornecer todos os requisitos projeto, bem como os recursos necessários para a execução. É importante que a CONTRATADA use de comunicações através de reuniões com a equipe técnica que executará o projeto;

11.18.1.2. Nesta fase deverá haver um pré-kickoff de projeto, com o objetivo de apresentar as equipes envolvidas no projeto e esclarecer dúvidas sobre escopo dos serviços previsto no

Termo de Referência, definir papéis e responsabilidades e esclarecer qualquer outro ponto relevante sobre a execução e medição do projeto.

11.18.2. Planejamento

11.18.2.1. Esta fase deverá ser realizada em até 15 (quinze) dias, contados da data de finalização da última fase, e deverá ser composta de:

11.18.2.2. Apresentação do Termo de Abertura do Projeto com matriz de responsabilidades, riscos envolvidos;

11.18.2.3. Apresentação do cronograma analítico do projeto com os responsáveis por executar cada atividade, estimativa de datas e períodos de execução, etapas e atividades;

11.18.2.4. Apresentação do plano de integrações que serão realizadas entre as plataformas do fabricante e os demais ativos da CONTRATANTE;

11.18.2.5. A CONTRATANTE designará um responsável técnico para ser o facilitador entre as áreas técnicas da CONTRATANTE, que providenciará os acessos, integrações e ações de preparação necessárias de serem realizadas nos ativos de sustentação da CONTRATANTE, para integrar as tecnologias que serão monitoradas.

11.18.3. Execução

11.18.3.1. Esta fase deverá ser realizada em até 15 (quinze) dias, contados da data de finalização da última fase, e deverá ser composta de:

11.18.3.1.1. Instalação dos Appliances que compõem a solução;

11.18.3.1.2. Configuração dos ativos e consoles que compõem a solução;

11.18.3.1.3. Filtragem dos logs de eventos de segurança;

11.18.3.1.4. Confecção de dashboards ou ativação de dashboards padrão;

11.18.3.1.5. Confecção de relatórios ou ativação de relatórios padrão;

11.18.3.1.6. Instalação de agentes de segurança necessários;

11.18.3.1.7. Criação dos casos de uso conforme descritos no termo de referência.

11.18.4. Encerramento

11.18.4.1. Esta fase deverá ser realizada em até 7 (sete) dias:

11.18.4.1.1. Revisão de todos os pontos da execução;

11.18.4.1.2. Confirmação das integrações realizadas conforme previsto no cronograma do projeto e escopo do edital;

11.18.4.1.3. Emissão do relatório de medição e termo de encerramento do projeto.

12. ITEM 12 - INSTALAÇÃO E CONFIGURAÇÃO DE GERENCIAMENTO CENTRALIZADO DE NGFW

12.1. Todas as fases de planejamento, instalação e configuração deverão ser realizadas com a presença de técnicos da CONTRATADA, que deverão possuir capacidade técnica necessária à execução do serviço;

12.2. Os trabalhos deverão ser realizados dentro do horário comercial, das 08:00 às 18:00, salvo casos em que necessite parada no ambiente que demande janelas de manutenção. Neste último caso, deve ser negociado os horários com antecedência;

12.3. Deve ser realizado previamente ao início dos trabalhos uma análise da topologia e arquitetura da rede, considerando os demais equipamentos de segurança do ambiente da CONTRATANTE;

12.4. Toda a instalação e configurações a serem realizadas devem ser de acordo com as melhores práticas do fabricante;

12.5. Este serviço deverá incluir:

12.5.1. Configuração e Parametrização lógica da solução contratada;

12.5.2. Projeto de configuração, contemplando todas as informações de ativação;

12.5.3. Após a instalação dos ativos físicos, atividades de integrações e customizações poderão ser realizadas de forma física e remota.

12.6. Criação de Template de configuração;

12.7. Deverá ser ministrado um treinamento do tipo “Repasse de conhecimento” para operação da Solução com duração de até 08 (oito) horas;

12.8. Deverá ser entregue documentação detalhada ao final da realização dos trabalhos contendo o passo-a-passo de toda instalação e configuração dos equipamentos envolvidos no projeto;

12.9. A instalação deverá ser dividida nas seguintes etapas:

12.9.1. Análise de Requisitos

12.9.1.1. Nesta fase a CONTRATADA terá até 7 (sete) dias para inventariar e fornecer todos os requisitos projeto, bem como os recursos necessários para a execução. É importante que a CONTRATADA use de comunicações através de reuniões com a equipe técnica que executará o projeto;

12.9.1.2. Nesta fase deverá haver um pré-kickoff de projeto, com o objetivo de apresentar as equipes envolvidas no projeto e esclarecer dúvidas sobre escopo dos serviços previsto no Termo de Referência, definir papéis e responsabilidades e esclarecer qualquer outro ponto relevante sobre a execução e medição do projeto.

12.9.2. Planejamento

12.9.2.1. Esta fase deverá ser realizada em até 7 (sete) dias, contados da data de finalização da última fase, e deverá ser composta de:

12.9.2.1.1. Apresentação do Termo de Abertura do Projeto com matriz de responsabilidades, riscos envolvidos;

12.9.2.1.2. Apresentação do cronograma analítico do projeto com os responsáveis por executar cada atividade, estimativa de datas e períodos de execução, etapas e atividades;

12.9.2.1.3. Apresentação do plano de integrações que serão realizadas entre as plataformas do fabricante e os demais ativos da CONTRATANTE;

12.9.2.2. A CONTRATANTE designará um responsável técnico para ser o facilitador entre as áreas técnicas da CONTRATANTE, que providenciará os acessos, integrações e ações de preparação necessárias de serem realizadas nos ativos de sustentação da CONTRATANTE, para integrar as tecnologias que serão monitoradas.

12.9.3. Execução

12.9.3.1. Esta fase deverá ser realizada em até quinze (quinze) dias, contados da data de finalização da última fase, e deverá ser composta de:

12.9.3.1.1. Instalação dos Appliances Virtuais que compõem a solução;

12.9.3.1.2. Configuração dos ativos e consoles que compõem a solução;

12.9.3.1.3. Filtragem dos logs de eventos de segurança;

12.9.3.1.4. Confecção de dashboards ou ativação de dashboards padrão;

12.9.3.1.5. Confecção de relatórios ou ativação de relatórios padrão;

12.9.3.1.6. Instalação de agentes de segurança necessários;

12.9.3.1.7. Criação dos casos de uso conforme descritos no termo de referência.

12.9.4. Encerramento

12.9.4.1. Esta fase deverá ser realizada em até 7 (sete) dias:

12.9.4.1.1. Revisão de todos os pontos da execução;

12.9.4.1.2. Confirmação das integrações realizadas conforme previsto no cronograma do projeto e escopo do edital;

12.9.4.1.3. Emissão do relatório de medição e termo de encerramento do projeto.

13. ITEM 13 - INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO DE ARMAZENAMENTO E AUDITORIA DE LOGS

13.1. Instalação e Configuração

13.1.1. Todas as fases de planejamento, instalação e configuração deverão ser realizadas com a presença de técnicos da CONTRATADA, que deverão possuir capacidade técnica necessária à execução do serviço;

13.1.2. Os trabalhos deverão ser realizados dentro do horário comercial, das 08:00 às 18:00, salvo casos em que necessite parada no ambiente que demande janelas de manutenção. Neste último caso, deve ser negociado os horários com antecedência;

13.1.3. Deve ser realizado previamente ao início dos trabalhos uma análise da topologia e arquitetura da rede, considerando os demais equipamentos de segurança do ambiente da CONTRATANTE;

13.1.4. Toda a instalação e configurações a serem realizadas devem ser de acordo com as melhores práticas do fabricante;

13.1.5. Este serviço deverá incluir:

13.1.5.1. Configuração e Parametrização lógica da solução contratada;

13.1.5.2. Projeto de configuração, contemplando todas as informações de ativação;

13.1.5.3. Após a instalação dos ativos físicos, atividades de integrações e customizações poderão ser realizadas de forma física e remota.

13.1.6. Criação de Template de configuração;

13.1.7. Deverá ser ministrado um treinamento do tipo “Repasse de conhecimento” para operação da Solução com duração de até 08 (oito) horas;

13.1.8. Deverá ser entregue documentação detalhada ao final da realização dos trabalhos contendo o passo-a-passo de toda instalação e configuração dos equipamentos envolvidos no projeto;

13.1.9. A instalação deverá ser baseada em um projeto executivo dividido nas seguintes etapas:

13.1.9.1. **Análise de Requisitos**

13.1.9.1.1. Nesta fase a CONTRATADA terá até 15 (quinze) dias para inventariar e fornecer todos os requisitos projeto, bem como os recursos necessários para a execução. É importante que a CONTRATADA use de comunicações através de reuniões com a equipe técnica que executará o projeto;

13.1.9.1.2. Nesta fase deverá haver um pré-kickoff de projeto, com o objetivo de apresentar as equipes envolvidas no projeto e esclarecer dúvidas sobre escopo dos serviços previsto no Termo de Referência, definir papéis e responsabilidades e esclarecer qualquer outro ponto relevante sobre a execução e medição do projeto.

13.1.9.2. **Planejamento**

13.1.9.2.1. Esta fase deverá ser realizada em até 15 (quinze) dias, contados da data de finalização da última fase, e deverá ser composta de:

13.1.9.2.1.1. Apresentação do Termo de Abertura do Projeto com matriz de responsabilidades, riscos envolvidos;

13.1.9.2.1.2. Apresentação do cronograma analítico do projeto com os responsáveis por executar cada atividade, estimativa de datas e períodos de execução, etapas e atividades;

13.1.9.2.1.3. Apresentação do plano de integrações que serão realizadas entre as plataformas do fabricante e os demais ativos da CONTRATANTE;

13.1.9.2.2. A CONTRATANTE designará um responsável técnico para ser o facilitador entre as áreas técnicas da CONTRATANTE, que providenciará os acessos, integrações e ações de preparação necessárias de serem realizadas nos ativos de sustentação da CONTRATANTE, para integrar as tecnologias que serão monitoradas.

13.1.9.3. <u>Execução</u>

13.1.9.3.1. Esta fase deverá ser realizada em até 30 (trinta) dias, contados da data de finalização da última fase, e deverá ser composta de:

13.1.9.3.1.1. Instalação dos Appliances que compõem a solução;

13.1.9.3.1.2. Configuração dos ativos e consoles que compõem a solução;

13.1.9.3.1.3. Filtragem dos logs de eventos de segurança;

13.1.9.3.1.4. Confecção de dashboards ou ativação de dashboards padrão;

13.1.9.3.1.5. Confecção de relatórios ou ativação de relatórios padrão;

13.1.9.3.1.6. Instalação de agentes de segurança necessários;

13.1.9.3.1.7. Criação dos casos de uso conforme descritos no termo de referência.

13.1.9.4. <u>Encerramento</u>

13.1.9.4.1. Esta fase deverá ser realizada em até 15 (quinze) dias:

13.1.9.4.1.1. Revisão de todos os pontos da execução;

13.1.9.4.1.2. Confirmação das integrações realizadas conforme previsto no cronograma do projeto e escopo do edital;

13.1.9.4.1.3. Emissão do relatório de medição e termo de encerramento do projeto.

14. ITEM 14 - MÓDULO TRANSCEPTOR SFP-10G-SR

14.1. O módulo transceptor ofertado, deve ser compatível ou fornecido pelo mesmo fabricante da solução ofertada, com o intuito de garantia da funcionalidade e compatibilidade;

14.2. Deve suportar o padrão 10GBASE-SR SFP+ (10GbE);

14.3. Suportar fibra ótica do tipo multimodo;

14.4. O módulo transceptor ofertado, deve possuir garantia mínima de 60 (sessenta) meses para troca, pelo fabricante ou pela empresa licitante;

14.5. Devem ser fornecidos, transceivers e cordões de fibra (OM3) para "Uplinks", totalmente compatíveis com os Switches CISCO em Produção (conforme quantitativos desse item).

15. ITEM 15 - MÓDULO TRANSCEPTOR SFP-10G-BASE-T

15.1. O módulo transceptor ofertado, deve ser compatível ou fornecido pelo mesmo fabricante da solução ofertada, com o intuito de garantia da funcionalidade e compatibilidade;

15.2. Deve suportar o padrão 10GBASE-T SFP (10GbE);

15.3. Deve suportar taxa de transferência de 100/1000/10000 Mbps;

15.4. O módulo transceptor ofertado, deve possuir garantia mínima de 60 (sessenta) meses para troca, pelo fabricante ou pela empresa licitante;

15.5. Devem ser fornecidos transceivers totalmente compatíveis com os Switches CISCO em Produção (conforme quantitativos desse item);

15.6. Devem ser fornecidos cabos UTP's (ao menos 10 metros), para "Uplinks" nos Switches em produção.

16. CARACTERÍSTICAS GERAIS PARA OS EQUIPAMENTOS NGFW (TIPOS 1, 2, 3 E 4)

16.1. Características operacionais

16.1.1. Deve possuir recurso de reversão do sistema operacional, e possuir pelo menos duas cópias de firmware na memória flash do sistema;

16.1.2. Deve salvar 10 (dez) versões do arquivo de configuração;

16.1.3. Deve possuir recurso para a exportação das configurações do ambiente de produção e de versões anteriores armazenadas em backup interno, para locais externos, sendo esses ao menos, servidor FTP, TFTP e o flash USB;

16.1.4. Deve possibilitar a configuração do protocolo de monitoramento SNMP v1, v2 e v3;

16.1.5. Deve possuir interface de Administração, por meio de acesso Web (WebUI) e linha de comando (CLI);

16.1.6. O acesso a interface de Gerenciamento deve utilizar minimamente os protocolos HTTPS, SSH, Telnet e Console direta por meio de porta especifica;

16.1.7. Deve possuir ao menos 3 (três) Perfis de Administrador do Sistema, incluindo "Administrador (permissão total), Operador (autoridade sobre as regras e políticas de firewall, exceto permissões do Administrador) e Auditor (visualiza configurações e logs de auditoria)";

16.1.8. Deve ser capaz de proteger o sistema de ataques do tipo: Força Bruta, utilizando no nome de usuário e senha;

16.1.9. Deve suportar política de segurança de senha para contas de Administração;

16.1.10. Deve possuir recurso para implantação rápida instalando automaticamente via USB, executando scripts locais e remotos;

16.1.11. Deve suportar o REST API para catálogo de endereços IP, AV, IPS, NAT, regra da política, interface, zona de segurança, roteamento e gerenciamento de atualizações;

16.1.12. Deve possuir gerenciamento local (console do equipamento), físico (hardware de gerenciamento) ou virtual (software de gerenciamento), não será aceito gerenciamento em nuvem pública;

16.1.13. Possuir garantia de 60 (sessenta) meses;

16.1.14. O fabricante ou o equipamento deve possuir pelo menos um dos seguintes certificados: ICSA (International Computer Security Association), ou CC (Common Criteria), ou pela Netsecopen.org;

16.1.15. Devem ser homologados na ANATEL.

16.2. Serviços de Rede

16.2.1. Deve possuir protocolos de roteamento dinâmico OSPF, BGP, RIPv2 e IS-IS;

16.2.2. Deve possuir o roteamento estático e o roteamento baseado em políticas (Policy Based Routing);

16.2.3. Deve possuir roteamento baseado em aplicativos, a fim de rotear aplicativos com P2P e vídeo on-line, com números dinâmicos de porta para o link WAN selecionado;

16.2.4. Deve possuir o roteamento ou o modo de operação NAT;

16.2.5. Deve ser compatível com o modo de operação transparente (bridge);

16.2.6. Deve possuir o modo de operação misto (NAT, Roteamento e Bridge);

16.2.7. Deve possuir os seguintes modos de interface:

16.2.7.1. Sniffer;

16.2.7.2. Port Aggregation;

16.2.7.3. Loopback;

16.2.7.4. VLANs (802.1q e Trunking).

16.2.8. Deve suportar comutação (switching) de camada 2 e roteamento em Camada 3;

16.2.9. Deve possuir o recurso de comutação (switch) virtual, cada comutador (switch) virtual deve ter sua própria tabela de endereços MAC;

16.2.10. Deve possuir recurso de roteamento virtual, cada roteador virtual deve ter sua própria tabela de roteamento;

16.2.11. Deve possuir o recurso de duplicação de tráfego na porta configurada para análise de tráfego, podendo ser baseada em IP de origem, IP de destino, porta de origem, porta de destino, protocolos de rede (TCP, UDP e/ou ICMP), entre outros. O espelho da porta pode ser configurado para entrada de tráfego, tráfego de saída ou ambos;

16.2.12. Deve possuir os recursos de SNAT, DNAT e PAT;

16.2.13. Deve permitir a configuração de NAT por política e configuração central de tabela NAT;

16.2.14. Deve possuir o recurso de NAT dinâmico e NAT estático, multi-para-um, um-para-multi NAT e um-para-um NAT;

16.2.15. Deve possuir o recurso de NAT444 (CGNAT) e a exportação da tabela de mapeamento estático NAT444 como um arquivo;

16.2.16. Deve possuir o recurso detecção de encaminhamento bidirecional (BFD), interação BFD com rota estática, OSPF e/ou BGP;

16.2.17. Deve possuir o recurso de expansão do grupo NAT para um endereço IPv4 público para suportar mais de 64 (sessenta e quatro) mil endereços IP privados;

16.2.18. Deve possuir os recursos de NAT46, NAT64 e DNS64;

16.2.19. Deve possuir o recurso de Full Cone NAT e STUN;

16.2.20. Deve possuir o recurso NetFlow, o dispositivo pode coletar o tráfego na entrada do usuário e enviá-lo para o servidor com a ferramenta de análise de dados NetFlow, para detectar, monitorar e coletar tráfego;

16.2.21. Deve possuir o recurso de visualização de informações do status do link de várias interfaces simultaneamente para análise comparativa;

16.2.22. Deve identificar o comportamento de acesso compartilhado na rede.

16.3. Características de Firewall

16.3.1. Deve possuir um objeto (entidade) predefinido e personalizável, permitindo ainda suportar o agrupamento de objetos;

16.3.2. Deve possuir recursos de política de segurança baseada em aplicação, função do usuário e a localização geográfica;

16.3.3. Deve possuir recursos de Camada de Saída de Aplicação, (ALG – Application Layer Gateway) ao menos os seguintes protocolos: MSRCP, PPTP, RAS, RSH, RTSP, SIP, SQLNetV2, SUNRPC, FTP, TFTP, HTTP, DNS-TCP, DNS-UDP, H.245, H.323, Q.931 e XDMCP;

16.3.4. Deve ser compatível com NAT46, NAT64, NAT444, SNAT, DNAT, PAT, Full Cone NAT e STUN;

16.3.5. Deve permitir a criação de uma “política única” para controle de aplicação, usuário autenticado, prevenção de ameaças, antivírus e filtragem de arquivos;

16.3.6. Deve suportar a verificação da redundância da política de segurança;

16.3.7. Deve suportar a contagem de utilização das políticas na WebUI;

16.3.8. Deve suportar a pesquisa de políticas na WebUI;

16.3.9. Deve suportar política programada, única e/ou recorrente;

16.3.10. Deve permitir configurar um grupo de políticas através do WebUI;

16.3.11. Deve possuir a configuração do limite de sessão com base no IP de origem, IP de destino, aplicação ou protocolo de aplicação (mysql, ms-sql, sqlnet, download P2P, vídeo, jogo, entre outros) e limitar novas conexões, sessões simultâneas;

16.3.12. Deve identificar e proteger de ataques de protocolos anormais, presentes no tráfego da rede;

16.3.13. Deve identificar e proteger de ataques a Tabela ARP;

16.3.14. Deve possuir proteção contra tipos de DDoS: inundações de consulta DNS, inundações de SYN, inundações de UDP, inundações de ICMP, Death Ping, Smurf, WinNuke e TCP Split Handshake; a ação suportada inclui registro e reset de sessão;

16.3.15. Deve possuir recursos para configurações para diferentes zonas de segurança.

16.4. Características de IPS

16.4.1. Deve possuir recurso para criar assinaturas personalizadas, atualizações automáticas de inserção ou extração de assinaturas, e uma enciclopédia de ameaças incorporada;

16.4.2. Deve possuir recursos de proteção contra injeção SQL, ataques DC e XSS;

16.4.3. Deve possuir proteção tráfego de C&C por meio de limite de solicitação, limite de proxy, limite personalizado e métodos amigáveis aos administradores;

16.4.4. Deve permitir 4 métodos de autenticação HTTP: Sem autenticação, JS Cookie, Redirecionar, Access Confirm e CAPCHA;

16.4.5. Deve possuir recurso de detecção de anomalias de protocolo, detecção rate-based;

16.4.6. Deve possuir as seguintes ações de IPS:

16.4.6.1. Default;

16.4.6.2. Monitoramento;

16.4.6.3. Bloqueio;

16.4.6.4. Reset (IP do invasor, IP da vítima ou interface de entrada) com tempo de expiração.

16.4.7. Os perfis de segurança do IPS devem ser definidos com base na gravidade, sistema operacional, aplicação e/ou protocolo;

16.4.8. Deve possuir recurso para isenção de IP de assinaturas IPS específicas;

16.4.9. Deve possuir o modo de operação “Sniffer IDS”;

16.4.10. Deve possuir o recurso de proteção DoS rate-based para IPv4 e IPv6 com configurações de limiar contra ataques de TCP Syn Flood, TCP/UDP/SCTP port scan, ICMP Sweep e Session Flooding para TCP/UDP/SCIP/ICMP (Origem/Destino);

16.4.11. Deve possuir recurso para configuração predefinida de perfis IPS;

16.4.12. Deve possuir recursos de Reputação IP para bloqueio de IPs de servidores botnet, fazendo uso de um banco de dados global de reputação de IPs;

16.4.13. Deve filtrar assinaturas de IPS, buscando por CVE ID;

16.4.14. Deve permitir que as atualizações de assinaturas sejam aplicadas por meio de um Sistema de Gerenciamento.

16.5. Características de Antivírus

16.5.1. Deve possuir o recurso de Antivírus baseado em fluxo de rede, sobre os protocolos HTTP, SMTP, POP3, IMAP e FTP/SFTP;

16.5.2. Deve suportar a detecção de vírus para arquivos compactados como RAR, ZIP, GZIP, BZIP2 e TAR;

16.5.3. Deve possuir recurso para a detecção de arquivos compactados em várias camadas, no mínimo 5 (cinco) camadas de descompressão e personalizar a ação para quando superar os comportamentos;

16.5.4. Deve possuir recurso de ações personalizadas para arquivos criptografados;

16.5.5. Deve possuir ao menos 2 (duas) das 3 (três) ações quando um vírus ou site malicioso for detectado:

16.5.5.1. Na ação de tratamento de arquivos infectados, a sobrescrita ou alteração do conteúdo do arquivo para inutilizá-lo, além de opções de bloqueio e registro de log;

16.5.5.2. Reset de conexão;

16.5.5.3. Gerar Log.

16.5.6. Deve possuir recurso de alerta ou advertência de possível código malicioso, para o usuário durante o acesso a um Site de Internet suspeito.

16.6. Características do Filtro de URL

16.6.1. Deve possuir a inspeção de filtro Web baseado em fluxo;

16.6.2. Deve possuir filtro Web definido manualmente com base em URL, conteúdo da Web e cabeçalho MIME;

16.6.3. Deve possuir os seguintes recursos adicionais de filtro da Web:

16.6.3.1. Filtro Java Applet, ActiveX e/ou Cookie;

16.6.3.2. Bloquear o Post HTTP;

16.6.3.3. Gerar log de palavras-chave de pesquisas;

16.6.3.4. Exceção à digitalização de conexões criptografadas em determinadas categorias para privacidade.

16.6.4. Deve permitir a substituição do perfil de filtro de URL, para que o administrador possa atribuir temporariamente diferentes perfis ao usuário/grupo/IP;

16.6.5. Deve permitir a personalização da página de aviso para filtro de URL;

16.6.6. Deve permitir a configuração de filtro de URL com base na zona de segurança.

16.7. Características do Sandbox na nuvem

16.7.1. Deve possuir recurso para envio de arquivos identificados como suspeitos/maliciosos para análise em ambiente computacional externo (cloud), objetivando efetuar testes de segurança no artefato, sem causar qualquer impacto ou dano ao ambiente computacional local;

16.7.2. Deve possuir recurso de envio de arquivos identificados como suspeitos oriundos de conexões de protocolos que incluem HTTP/HTTPS, POP3, IMAP, SMTP, SMB e FTP, objetivando efetuar testes de segurança no artefato, sem causar qualquer impacto ou dano ao ambiente computacional local;

16.7.3. Deve permitir a inspeção de arquivos dos tipos: PE, ZIP, RAR, Office, PDF, APK, JAR e SWF;

16.7.4. Deve permitir definir o tamanho limite do arquivo a ser enviado para a Sandbox;

16.7.5. Deve possibilitar a geração de um relatório abrangente de análise comportamental para arquivos maliciosos;

16.7.6. Deve possuir recurso onde utilize resultados de detecção para bloquear uma ameaça desconhecida rapidamente;

16.7.7. Deve possuir recurso de consulta ao compartilhamento global de inteligência e bloqueio de ameaças em "tempo real", provido pelo Fabricante da Solução.

16.8. Características de Prevenção Botnet – Comando e Controle (C&C)

16.8.1. Deve ser capaz de identificar atividades de máquinas infectadas com sistemas de automação de tarefas (botnet) na intranet, neutralizando novos ataques avançados dessas ameaças, comparando as informações obtidas com o banco de dados de endereços C&C (Comando e Controle);

16.8.2. Deve suportar atualizações regulares de endereços de servidores de Botnet hospedados na internet;

16.8.3. Deve suportar 2 (dois) tipos de banco de dados de endereços C&C: O banco de dados de endereços IP e o banco de dados de domínios;

16.8.4. Deve possuir recurso de descoberta dos protocolos TCP, HTTP e DNS;

16.8.5. Deve permitir a criação de uma Lista de Endereços Autorizados (White List) de C&C (IPs e domínios).

16.9. Características de Reputação IP

16.9.1. Deve possuir a capacidade de filtrar o tráfego de endereços IPs de baixa reputação, incluindo Botnet, Spam, módulos comprometidos, força bruta, entre outros;

16.9.2. Deve possuir recurso para registrar, excluir e/ou bloquear pacotes se o tráfego mal-intencionado atingir a lista de reputação IP;

16.9.3. Deve possuir recursos de atualização do banco de dados de Reputação de Endereços IPs;

16.9.4. Deve possuir recurso de filtragem de endereço IP de bots e servidores de Botnet.

16.10. Características de Descriptografia SSL/TLS

16.10.1. A Solução deve ser capaz de inspecionar o tráfego SSL/TLS, permitindo identificar dados e informações que não estejam de acordo com as Políticas de Segurança;

16.10.2. Deve possuir recurso de identificação da aplicação no tráfego criptografado SSL/TLS;

16.10.3. Deve possuir recursos de IPS para inspeção do tráfego criptografado SSL/TLS;

16.10.4. Deve possuir recursos de Antivírus para inspeção do tráfego criptografado SSL/TLS;

16.10.5. Deve possuir módulo para inspeção da transferência de arquivos no tráfego criptografado SSL/TLS;

16.10.6. A inspeção do tráfego SSL/TLS deve suportar a configuração de acordo com a política de firewall especifica, e não como Configuração global (após vincular o perfil proxy SSL a uma regra de política, o sistema deve processar o tráfego que corresponde a regra, de acordo com a configuração do perfil).

16.11. Características de Identificação e Controle

16.11.1. A solução deve suportar a identificação de Windows, Linux, IOS, Android, entre outros;

16.11.2. Deve possuir recurso de consultas baseadas em IP e número de dispositivos;

16.11.3. Deve possuir recursos para a visualização da descrição, fatores de risco, dependências, portas típicas usadas, URLs para referências adicionais e informações para cada aplicação no WebUI;

16.11.4. Deve possuir recurso de bloqueio, reinicialização, monitoramento e configuração de tráfego para aplicações;

16.11.5. Deve ser capaz de identificar e controlar aplicações em nuvem, fornecer monitoramento multidimensional e estatísticas para essas aplicações, incluindo categoria de risco;

16.11.6. Deve possuir controle de transferência de arquivos nos protocolos HTTP, HTTPS, FTP, SMTP e POP3; IMAP;

16.11.7. Deve possuir recurso de filtragem de conteúdo para os protocolos HTTP-GET, HTTP-POST, FTP e SMTP;

16.11.8. Deve possuir banco de dados de usuários local;

16.11.9. Deve possuir autenticação do usuário com TACACS+, LDAP, Radius e Active Directory;

16.11.10. Deve possuir a interação com sistema de autenticação de terceiros através de API aberta;

16.11.11. Deve possuir autenticação de 2 (dois) fatores, seja com suporte de terceiros, servidor de Token integrado e/ou SMS;

16.11.12. Deve possuir a sincronização de grupos de usuários baseado em Active Directory e LDAP;

16.11.13. Deve possuir recursos de autenticação 802.1x e SSO Proxy;

16.11.14. Deve possuir recursos de personalizar a página de autenticação da Web;

16.11.15. Deve possuir autenticação ativa baseada em interface Web;

16.11.16. Deve possuir recurso de um único login: Windows AD, Agentless AD SSO Role (AD Pooling);

16.11.17. Deve possuir recurso para utilizar o protocolo de monitor SSO para sincronização de usuários autorizados;

16.11.18. Deve possuir o recurso de WebAuth baseado em MAC.

16.12. Características de QoS

16.12.1. Deve possuir controle máximo ou garantido de largura de banda em um endereço IP ou usuário;

16.12.2. Deve possuir recursos de tunelamento com base no domínio de segurança, interface, endereço, usuários e/ou grupo de usuários, servidores e/ou pool de servidores, aplicações e/ou pool de aplicações, TOSs e VLANs;

16.12.3. Deve possuir controle de largura de banda alocada por tempo, prioridade ou a mesma largura de banda compartilhada;

16.12.4. Deve possuir recursos de TOS e DiffServ;

16.12.5. Deve possuir recursos para configurar políticas de QoS programadas por horários específicos;

16.12.6. Deve suportar a alocação flexível e priorizada da largura de banda restante (não usada);

16.12.7. Deve possuir recurso de alocação de largura de banda com base na categoria de URL;

16.12.8. Deve possuir recursos compatíveis com endereços IPv6 na função QoS;

16.12.9. O monitor deve suportar a exibição de tendências de tráfego, tráfego de download e tráfego total para todos os túneis ou sub-túneis (entende-se como túnel para o objeto de controle de tráfego em QoS).

16.13. Características do Balanceamento de Servidores

16.13.1. Deve suportar o Balanceamento de Carga do Servidor (SLB – Server Load Balancing);

16.13.2. Deve possuir o recurso de algoritmos SLB: Hashing ponderado, menor conexão ponderada e round-robin;

16.13.3. Deve possuir proteção de sessão, persistência de sessão e monitoramento do status da sessão;

16.13.4. Deve possibilitar a verificação da saúde do servidor, o monitoramento da sessão e a proteção da sessão.

16.14. Características do Balanceamento de Links

16.14.1. Deve suportar o balanceamento de LINK bidirecional;

16.14.2. Deve suportar balanceamento de LINK bidirecional de saída, incluindo roteamento baseado em políticas, ECMP e pesos, roteamento de ISP incorporado e detecção dinâmica de qualidade do link;

16.14.3. Deve suportar balanceamento de LINK bidirecional de entrada, compatível com DNS e detecção dinâmica de qualidade do link;

16.14.4. Deve suportar a comutação automática de link com base na largura de banda, latência, jitter, conectividade e aplicação;

16.14.5. Deve suportar a proteção contra sobrecarga de link, o tráfego deverá mudar para outro link quando o atual estiver sobrecarregado. O sistema deve continuar monitorando a largura de banda dos links e bloquear novas sessões para o link que está sobrecarregado de acordo com as configurações;

16.14.6. Deve suportar a inspeção estatal de link com ARP, PING e DNS.

16.15. Características de VPN

16.15.1. Deve possuir os seguintes recursos de VPN IPSec:

16.15.1.1. Modo IPSec Fase 1: modo de proteção agressivo e principal;

16.15.1.2. Compatível com IKEv1 e IKEv2 (RFC 4306);

16.15.1.3. Método de autenticação: certificado e chave pré-compartilhada;

16.15.1.4. Suportar a configuração no modo IKE (servidor e cliente);

16.15.1.5. Fase 1 / Fase 2 de criptografia: DES, 3DES, AES128, AES192 e AES256;

16.15.1.6. Fase 1 / Fase 2 de autenticação: MD5, SHA1, SHA256, SHA384 e SHA512;

16.15.1.7. Fase 1 / Fase 2 Suporte Diffie-Hellman: 1,2 e 5;

16.15.1.8. XAuth como modo servidor e para usuários dial-up;

16.15.1.9. Autokey manter-se ativo para a Fase 2 SA;

16.15.2. Deve possuir recursos de VPN IPSec baseada em rotas e políticas;

16.15.3. Deve possuir os seguintes modos de implantação da VPN IPSec:

16.15.3.1. Gateway para Gateway;

16.15.3.2. Full-mesh;

16.15.3.3. Hub e Spoke;

16.15.3.4. Túnel redundante;

16.15.3.5. Terminação VPN no modo transparente.

16.15.4. Deve possuir recursos de VPN SSL para Linux, iOS, Android e Windows XP/Vista/7/10/11, incluindo sistemas operacionais Windows de 64 bits;

16.15.5. Deve possuir recursos de VPN SSL com um único login, impedindo logins simultâneos com o mesmo nome de usuário;

16.15.6. Deve possuir recursos de Portal SSL com limite de usuários;

16.15.7. Deve possuir recursos de SSL, onde o módulo de encaminhamento da porta VPN deve criptografar os dados do cliente e enviar para o servidor da aplicação;

16.15.8. Deve possuir recursos de verificação de integridade do host e do sistema operacional antes da conexão do túnel SSL;

16.15.9. Deve possuir opção de limpeza de cache antes de encerrar a sessão da VPN SSL;

16.15.10. Deve permitir vários logins de VPN SSL personalizados, associados a grupos de usuários (url paths e design);

16.15.11. Deve possuir recursos de autenticação SSL com uma chave USB;

16.15.12. Deve possuir o modo de servidor e cliente L2TP, L2TP sobre IPSec, GRE sobre IPSec;

16.15.13. Deve possuir recursos de VPN para implantação rápida de Escritório Remoto, por meio de VPN site to site.

16.16. Características de IPv6

16.16.1. Deve possuir recursos de gerenciamento de dispositivos sobre IPv6, registro IPv6 e Alta disponibilidade (HA) no IPv6;

16.16.2. Deve possuir recursos de túneis IPv6, DNS64/NAT64, entre outros;

16.16.3. Deve possuir recursos de configuração de protocolos de roteamento IPv6 para roteamento estático, roteamento de políticas, ISIS, RIPng, OSPFv3 e BGP4+;

16.16.4. Deve possuir recursos de VPN IPSec para IPv6;

16.16.5. Deve possuir recursos de IPS IPv6, identificação de aplicações, filtragem de URL, Antivírus, controle de acesso e defesa de ataque ND;

16.16.6. Deve possuir recursos de conjunto estático, registro e monitoramento para IPv6;

16.16.7. Deve ser possuir recursos de configurar e bloquear endereços IPv6.

16.17. Características de Alta Disponibilidade (HA)

16.17.1. Deve ser compatível com os modos Ativo/Ativo e Ativo/Passivo;

16.17.2. Deve possuir recursos de configuração de interfaces de heartbeat redundantes para Alta Disponibilidade (HA);

16.17.3. Deve possuir recursos de sincronização de sessão autônoma;

16.17.4. Deve possuir recursos de failover de Alta Disponibilidade (HA) baseado em interface Web, HTTP, ICMP, ARP, DNS e rastreamento de objetos baseados em TCP;

16.17.5. Deve possuir recursos com as seguintes opções de implantação da Alta Disponibilidade (HA):

16.17.5.1. HA com agregação de links;

16.17.5.2. Malha completa HA;

16.17.5.3. HA geograficamente disperso.

16.17.6. Deve possuir recursos de Alta Disponibilidade (HA) no modo peer, para evitar problemas de roteamento assimétrico na implementação do modo Ativo/Ativo.

16.18. Características de Logs e Relatórios

16.18.1. Deve possuir o recurso de Syslog padrão e o registro de formato binário;

16.18.2. Deve efetuar o armazenamento de log binário distribuído para vários servidores de log, algoritmo distribuído suportando Round robin e/ou Src IP HASH;

16.18.3. Deve possuir o registro de logs em servidores de memória local ou syslog;

16.18.4. Deve possuir o recurso de envio de log no formato binário ou texto;

16.18.5. Deve possuir o recurso de transferência de logs sobre UDP, TCP e Secure-TCP;

16.18.6. Deve possuir o recurso de registro confiável usando a opção TCP (RFC 3195);

16.18.7. Deve apresentar pelo menos 3 (três) relatórios predefinidos: relatórios de segurança, fluxo e rede;

16.18.8. Deve possuir relatórios definidos pelo usuário, podendo ser exportado em PDF, por e-mail e/ou FTP;

16.19. Características de Monitoramento

16.19.1. Deve possuir o recurso de exibir estatísticas de tráfego de aplicações por usuário;

16.19.2. Deve possuir o recurso de monitoramento de estatísticas multidimensionais para aplicações baseado em riscos, categorias, recursos e tecnologia;

16.19.3. Deve exibir estatísticas para visitas de URL e categoria URL;

16.19.4. Deve exibir estatísticas de tráfego em “tempo real”;

16.19.5. Deve exibir estatísticas de eventos de segurança;

16.19.6. Deve possuir o recurso de monitoramento definido pelo usuário;

16.19.7. Deve possuir o recurso exportação de relatórios em formatos PDF, Word e/ou HTML;

16.19.8. Deve possuir o recurso de monitoramento do status do dispositivo, como CPU, memória, temperatura, entre outros;

16.19.9. Deve possuir o recurso de monitoramento centralizado para vários dispositivos, incluindo CPU, memória, tráfego, sessões, aplicações, usuários, ameaças, entre outros. Permitindo o acesso através de um aplicativo móvel, pelo menos dos últimos 7 (sete) dias:

16.19.9.1. O aplicativo de monitoramento deverá suportar acesso à Web e através de aplicativo(s) em dispositivos móveis;

16.19.9.2. O aplicativo de monitoramento deverá fornecer relatórios personalizados e agendados.

17. GARANTIA, ASSISTÊNCIA E SUPORTE TÉCNICO PARA SOLUÇÕES DE SOFTWARE E HARDWARE

17.1. Trata-se dos serviços de Garantia, Assistência técnica e Suporte Técnico pelo período de vigência contratual de 60 (sessenta) meses;

17.2. A Garantia, Assistência Técnica e Suporte Técnico do fabricante, devem ser contados a partir do recebimento definitivo do Objeto;

17.3. Deve estar identificado de forma clara na proposta os números de identificação dos produtos (Part Numbers) do fabricante referentes as garantias fornecidas;

17.4. Disponibilizar estrutura de suporte técnico por meio de atendimento telefônico, website e e-mail, na modalidade 24x7x365;

17.5. Os serviços compreendem:

17.5.1. Substituição de equipamentos e componentes decorrente de vícios de projeto, fabricação, construção e montagem;

17.5.2. Fornecimento de atualizações necessárias para a correção de vícios(bugs);

17.5.3. A atualização de sistema operacional dos equipamentos para obter novas funcionalidades e correções;

17.5.4. Disponibilizar todas as atualizações dos softwares e firmwares dos equipamentos, concebidas em data posterior ao seu fornecimento, pelo período mínimo de 60 (sessenta) meses, sem qualquer ônus adicional à CONTRATANTE;

17.5.5. Realizar a atualização das assinaturas de proteção da solução, se necessárias;

17.5.6. Permitir realizar consultas técnicas ou questionamentos da equipe da CONTRATANTE para sanar dúvidas, repassar conhecimentos, ou ainda obter melhores práticas;

17.5.7. Prever a reposição de peças e equipamentos, abrangendo todos os itens que compõem a solução, incluindo módulos ou outros equipamentos fornecidos para atendimento aos requisitos da aquisição;

17.6. Os serviços de garantia e de assistência técnica deverão ser prestados por técnicos devidamente habilitados e credenciados pelo fabricante, com nível de certificação compatível com as atividades a serem executadas, e sem qualquer ônus adicional;

17.7. Para a substituição de um equipamento/componente inoperante ou com falha no sistema, o atendimento deverá ser efetuado em 24 (vinte e quatro) horas;

17.7.1. Constatada a impossibilidade de recuperar o equipamento/componente sob um prazo máximo de 72 (setenta e duas) horas, após a abertura do chamado, o equipamento/componente com defeito deverá ser substituído por outro de igual capacidade e capaz de atender as mesmas funcionalidades, com prazo máximo de 30(trinta) dias, prorrogáveis por igual período;

17.8. O envio de equipamentos/componentes de reposição, deverão ser entregues nos locais especificados neste termo de referência, sendo todos os custos de deslocamento (envio e retorno) dos mesmos, de responsabilidade integral da CONTRATADA;

17.9. Todo o chamado aberto deve ter sua resolução técnica registrada no sistema de atendimento do fornecedor da solução;

17.9.1. O atendimento deve ser prestado em idioma local (português), sendo aceito atendimento em demais idiomas, desde que ocorra o acompanhamento técnico da

CONTRATADA, responsável pela mediação do contato, em todo o processo de atendimento do chamado.

ANEXO II (DO TERMO DE REFERÊNCIA) – MINUTA DOS TERMOS DO CONTRATO

Contrato de Fornecimento nº XXX/XXXX

Processo Administrativo nº XXXXXXX/XXXX

XXXXXXXXXX nº XXX/XXXX

CONTRATO DE FORNECIMENTO QUE CELEBRAM ENTRE SI O **MUNICÍPIO DE VITÓRIA** E A EMPRESA XXXXXXXXXXX.

O **MUNICÍPIO DE VITÓRIA**, por intermédio da **XXXXXXXXX,** órgão de direito público interno, inscrita no CNPJ sob o nº **XXXXXXXXX**, com sede à Av. XXXXXXXXXXXXXXX, nesta Capital, representada legalmente pelo **SECRETÁRIO MUNICIPAL DE XXXXXXXXXXXXXXXXXX,** Sr. **XXXXXXXXXXXXXXXX,** CPF n.º XXX.XXX.XXX-XX, adiante denominado **CONTRATANTE** e, de outro lado, a Empresa **XXXXXXXXXXXXXXXXX**, CNPJ nº XXXXXXXXXXX, estabelecida à Rua XXXXXXXXXXXXXXXXXXXXXX, tendo por seu representante legal, o Sr. **XXXXXXXXXXXXXXXXX**, CPF nº XXXXX doravante denominada **CONTRATADA**, celebram o presente contrato de **FORNECIMENTO**, nos termos da Lei 14.133/2021, e do **XXXXXXX nº XXX/XXXX**, oriundo do Processo Administrativo nº **XXXXXXX/XXXX**, que passa a fazer parte deste instrumento, independente de transcrição, juntamente com a Proposta Comercial apresentada pela CONTRATADA, ficando, porém, ressalvadas como não transcritas, as condições nela estipuladas que contrariem as disposições deste Contrato, que reger-se-á pelas cláusulas seguintes:

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. Constitui objeto do presente instrumento o **REGISTRO DE PREÇOS VISANDO FUTURA E EVENTUAL CONTRATAÇÃO DE EMPRESA PARA O FORNECIMENTO DE SOLUÇÃO DE FIREWALL DE PRÓXIMA GERAÇÃO (NEXT-GENERATION FIREWALL), INCLUINDO SERVIÇOS DE INSTALAÇÃO, CONFIGURAÇÃO, SUPORTE E GARANTIA** conforme descrição, quantidade e preços relacionados no Termo de Referência e seus anexos.

CLÁUSULA SEGUNDA – DO VALOR GLOBAL

2.1. O valor global do presente contrato é de **R$ xxxxxx (xxxxxxxxxxxxxxxxxxxxxx).**

2.2. No preço já estão inclusos todos os custos e despesas, inclusive transportes, taxas, impostos, seguros, licenças e outros relacionados ao fornecimento, bem como garantia, quando for o caso.

CLÁUSULA TERCEIRA – DA VIGÊNCIA DO CONTRATO

3.1. O prazo de vigência do contrato será 1825 (mil e oitocentos e vinte e cinco) dias consecutivos, a contar da data de sua assinatura, podendo ser prorrogado conforme o disposto no Art. 107, da Lei 14.133/2021, mediante Termo Aditivo, devidamente autorizada formalmente pela Autoridade Competente. O prazo para início do fornecimento se iniciará a partir do recebimento da Ordem de Serviços (OS) / Autorização de Fornecimento (AF).

3.1.1. Poderão ser prorrogados, conforme art. 107 da Lei 14.133/2021, mediante Termo Aditivo, devidamente autorizado formalmente pela Autoridade Competente, somente os itens listados abaixo:

ITEM	TIPO	CÓD. MAT. PMV	DESCRIÇÃO RESUMIDA	UNID	QTD
5	SW		Gerenciamento Centralizado de NGFW	UN	2
7	SE		Treinamento para Solução e Segurança	UN	2
8	SE		Serviço de operação assistida da solução de segurança	Mensal	60
9	SE		Serviço de suporte técnico 8x5	UN	360

12	SE		Instalação e Configuração de Gerenciamento Centralizado de NGFW	UN	2

Legendas: "**SW**" – Software; "**SE**" – Serviços.

3.2. Nos contratos assinados eletronicamente, será considerada a data da última assinatura.

3.3. A eficácia do mesmo dar-se-á após a publicação resumida do instrumento na Imprensa Oficial do Município de Vitória (art. 52 da Lei Orgânica) e no Portal Nacional de Contratações Públicas (PNCP).

CLÁUSULA QUARTA – DOS RECURSOS ORÇAMENTÁRIOS

4.1. As despesas decorrentes da presente contratação correrão à conta da Dotação Orçamentária: XX.XX.XX.XXX.XXXX.X.XXXX - Elemento de Despesa: X.X.XX.XX.XX - Fonte do Recurso: X.XXX.XXXX.XXXX.

CLÁUSULA QUINTA – DOS LOCAIS, PRAZOS E CONDIÇÕES DE ENTREGA

5.1. Homologada a licitação pela autoridade competente, em sendo realizada a contratação, será firmado Termo de Contrato ou emitido instrumento equivalente.

5.2. O licitante vencedor será convocado pela Administração, para assinar o Termo de Contrato ou para aceitar ou retirar o instrumento equivalente, no prazo de 05 (cinco) dias úteis a partir da data da convocação, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas neste Contrato e seus anexos.

5.3. O prazo para assinatura do contrato poderá ser prorrogado 1 (uma) vez, por igual período, mediante solicitação da parte durante seu transcurso, devidamente justificada e desde que o motivo seja aceito pela Administração.

5.4. A Administração, quando o convocado não assinar o Termo de Contrato ou não aceitar ou retirar o instrumento equivalente no prazo e nas condições estabelecidas, poderá convocar os licitantes remanescentes, na ordem de classificação, para a celebração do contrato nas condições propostas pelo licitante vencedor.

5.5. Caso nenhum dos licitantes aceitar a contratação nos termos do subitem anterior, a Administração, observados o valor estimado e sua eventual atualização nos termos deste Contrato, poderá:

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

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

5.6. A entrega do objeto da presente licitação dar-se-á no prazo máximo de 60 (sessenta) dias consecutivos, contados do recebimento da Autorização de Fornecimento (AF), em remessa única. No caso de Ordem de Serviços (OS), a CONTRATADA terá um prazo máximo de 30 (trinta) dias corridos para início da prestação dos serviços

5.7. A(s) entrega(s) deverá(ão) ser realizada(s) no(s) seguinte(s) endereço(s): **Subsecretaria de Tecnologia da Informação do Município de Vitória**, no endereço Rua Francisco Rubim, 169, Bento Ferreira, Vitória, ES, CEP 29050-680.

5.8. O horário de recebimento será das **09h às 16h**.

5.9. O local de fornecimento poderá sofrer alteração, a critério da administração, mediante prévia comunicação ao Fornecedor.

5.10. Os locais de instalação serão em qualquer localidade do Município de Vitória, sendo a definição feita pelo Fiscal do Contrato.

5.11. O fornecedor deverá atentar para o cumprimento dos prazos, sob pena de aplicação de sanção, em caso de atraso injustificado.

5.12. Os produtos deverão ter garantia mínima conforme especificação de cada item, contado a partir da data de emissão do termo de recebimento definitivo.

5.13. A entrega deverá acompanhar cópia da Autorização de Fornecimento (AF) ou a Nota Fiscal que deverá conter os dados principais do processo de aquisição (nº Processo, nº Licitação, nº AF) a fim de facilitar o recebimento do objeto e agilizar o processo de pagamento.

5.14. O fornecedor fará constar da nota fiscal os valores unitários e respectivos valores totais em conformidade com o constante da correspondente nota de empenho ou contrato, atentando para as inexatidões que poderão decorrer de eventuais arredondamentos.

5.15. O fornecedor deverá garantir a qualidade do objeto, devendo, ainda, quando solicitado, substituir prontamente o que porventura não atenda aos requisitos contratados, sob pena das sanções cabíveis.

5.16. O objeto será recebido provisoriamente, de forma sumária, pelo(a) responsável pelo acompanhamento e fiscalização da contratação, com verificação posterior da conformidade do material com as exigências constantes neste Termo de Referência e na proposta.

5.17. O recebimento provisório deverá ocorrer de forma imediata (no ato da entrega do objeto).

5.18. O objeto poderá ser rejeitado, no todo ou em parte, quando em desacordo com as especificações constantes neste Contrato e na proposta, devendo ser substituídos no prazo de 30 (trinta) dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

5.19. Os bens serão recebidos definitivamente, por servidor ou comissão designada, no prazo de até 15 (quinze) dias, contados do recebimento provisório, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo circunstanciado.

5.20. Na hipótese de a verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo.

5.21. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da contratada pelos prejuízos resultantes da incorreta execução da contratação.

5.22. Os prazos para os serviços de instalações e configurações conforme relacionados na “Tabela – Itens de Serviços do Lote”, considerando sua complexidade, deverão ser realizados, conforme tabela abaixo:

ITENS DE SERVIÇOS DO LOTE		
Item	***Descrição***	***Prazo Máximo***
10	Instalação e Configuração de NGFW Tipo 1 e 2	28 dias
11	Instalação e Configuração de NGFW Tipo 3 e 4	60 dias
12	Instalação e Configuração de Gerenciamento Centralizado de NGFW	34 dias
13	Instalação e Configuração Solução de Armazenamento e Auditoria de Logs	75 dias

Tabela – Itens de Serviços do Lote

5.23. Os prazos para os serviços de instalações e configurações conforme relacionados na "Tabela - Itens de Serviços sob demanda do Lote", deverão ser iniciados em até 05 (cinco) dias úteis considerando o recebimento de suas Ordens de Serviço (OS), exclusivamente para os itens:

ITENS DE SERVIÇOS AVULSOS DO LOTE	
Item	***Descrição***
08	Serviço de operação assistida da solução de segurança
09	Serviço de suporte técnico 8x5

Tabela – Itens de Serviços sob demanda do Lote

5.24. Para a realização do Item "Serviço: Treinamento para Solução e Segurança", este não deverá ultrapassar o prazo máximo de 120 (cento e vinte) dias após o recebimento da primeira Autorizações de Fornecimento (AF).

5.25. Para os Itens: instalação física dos bens e materiais (componentes de hardwares) adquiridos por meio deste certame, ocorrerão após mediante adequação da infraestrutura, tais como: espaço útil em "Rack" no ambiente de datacenter designado, energização e prover meio de passagem dos cabos adquiridos para a conectividade. Estes serviços serão de responsabilidade da equipe técnica designada da CONTRATANTE, e ainda:

5.25.1. Caberá à equipe técnica da CONTRATANTE, repassar e realizar todos os demais serviços contendo o repasse de informações e adequações da sua infraestrutura de conectividade lógica, visando a comportar os novas soluções e/ou componentes (hardwares e softwares) adquiridos através deste certame.

5.26. Para todos os Itens: após o recebimento de sua Autorização de Fornecimento (AF), bem como a assinatura do contrato, em um prazo de até 10 (dez) dias úteis, será realizada uma reunião com a equipe técnica designada, com o(s) profissional(is) designado(s) pela(s) CONTRATADA(S), com intuito de apresentar um resumo dos bens e serviços adquiridos, e ainda, propor um cronograma para a execução dos serviços contratados, onde nesta reunião, deverá apresentar de forma clara e resumida, as fases de execução dos serviços relacionados e contratados a partir deste certame.

CLÁUSULA SEXTA – DO ACOMPANHAMENTO E FISCALIZAÇÃO DO CONTRATO

6.1. A **Gestão** desta contratação será realizada pelo(a) servidor(a) **RODRIGO GIUBERTI BOITEUX**, e a **Fiscalização** será realizada pelos servidores **FERNANDO PAIVA BEZERRA** e **JOÃO PAULO MIRANDA COTA**, telefone (27) 3382-6325, ou por outro servidor designado por meio de Ato de Designação do Secretário da Pasta requisitante, nos termos do Art. 117, da Lei n.º 14.133/2021, que deverá atestar o recebimento dos materiais.

6.2. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios ocultos, e, na ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos.

6.3. O representante da Administração anotará em registro próprio todas as ocorrências relacionadas com a execução da contratação, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das falhas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

CLÁUSULA SÉTIMA – DAS CONDIÇÕES DE PAGAMENTO

7.1. O pagamento deverá ser solicitado pela CONTRATADA por meio da apresentação no Protocolo Virtual do Município de Vitória (protocolo.vitoria.es.gov.br) da Nota Fiscal ou documento de cobrança equivalente acompanhada da documentação prevista nesta cláusula.

7.2. A liquidação da despesa será realizada no prazo de até 10 (dez) dias úteis contados da emissão do Termo de Recebimento Definitivo do objeto.

7.2.1. Após a emissão do Termo de Recebimento Definitivo do objeto, o fiscal da contratação deverá encaminhar imediatamente (no mesmo dia) o processo para o setor responsável pela liquidação da despesa.

7.3. O pagamento será efetuado no prazo de até 07 (sete) dias úteis contados da finalização da liquidação da despesa.

7.4. Para atesto do fornecimento serão observados os seguintes aspectos:

a) Critério de Avaliação: FORNECIMENTO, para entrega de bens; EXECUÇÃO, para serviços técnicos.

b) Tipo de pagamento: ÚNICO quando da entrega de bens e POR DEMANDA quando da execução de serviços.

7.5. A(S) NOTA(S) FISCAL(IS) OU DOCUMENTO(S) DE COBRANÇA EQUIVALENTE(S) DEVERÁ(ÃO) SER EMITIDA(S) PARA CADA FONTE DE RECURSO, COM A RAZÃO SOCIAL, CNPJ E ENDEREÇO COMPLETO DO ÓRGÃO REQUISITANTE, CONSTANTES NA AUTORIZAÇÃO DE FORNECIMENTO.

7.6. Na emissão da Nota Fiscal, o fornecedor deverá descrever: o objeto, obrigatoriamente, em conformidade com a descrição contida em sua proposta; o número do processo que originou a contratação; número do contrato; número da Autorização de Fornecimento; e dados bancários, com indicação do banco, agência e conta.

7.7. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.

7.8. A Nota Fiscal ou Documento de cobrança equivalente deverá ser obrigatoriamente acompanhada dos documentos previstos no Edital, em conformidade com a Norma de Procedimento de Liquidação da Despesa.

7.9. Constatada a situação de irregularidade em quaisquer das certidões da CONTRATADA, ela será notificada, por escrito, sem prejuízo do pagamento pelo objeto já executado, para, num prazo de 05 (cinco) dias úteis, regularizar tal situação ou, no mesmo prazo, apresentar defesa, sob pena de rescisão contratual.

7.10. Os pagamentos poderão ser sustados pela Contratante nos seguintes casos:

I. Não cumprimento das obrigações assumidas que possam, de alguma forma, prejudicar o requisitante;

II. Inadimplência de obrigações assumidas pelo fornecedor para com o Município de Vitória, por conta do estabelecido neste Termo de Referência;

III. Erros ou vícios na(s) Nota(s) Fiscal(is)/Fatura(s).

7.11. É vedada a antecipação de pagamentos sem a contraprestação.

7.12. É expressamente vedado a contratada a cobrança ou desconto de duplicatas através de rede bancária ou de terceiros.

7.13. A CONTRATANTE poderá deduzir dos pagamentos importâncias que, a qualquer título, lhe forem devidas pelo fornecedor, em decorrência de inadimplemento das obrigações aqui assumidas, facultando o exercício do contraditório.

7.14. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, o valor devido deverá ser atualizado monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação da seguinte fórmula:

$$\mathbf{VM} = \mathbf{VP} \times \frac{\mathbf{I}}{\mathbf{360}} \times \mathbf{N}$$

Onde:

VM = Valor da multa financeira;

VP = Valor da nota fiscal referente ao mês em atraso;

I = IPCA-IBGE;

N = Número de dias em atraso.

CLÁUSULA OITAVA – DAS OBRIGAÇÕES DAS PARTES

8.1. DA CONTRATADA

8.1.1. A CONTRATADA deve cumprir todas as obrigações constantes neste Termo de Referência, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

8.1.1.1. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Termo de Referência e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo, procedência e prazo de garantia ou validade;

8.1.1.2. A contratada deverá fornecer todos os componentes (Equipamentos, cabos e demais acessórios, softwares e seus licenciamentos) que compõem a Solução ofertada, inclusive no que tange a prestação dos serviços ofertados conforme especificações técnicas e condições exigidas no Termo de Referência deste Edital, cujos custos deverão estar inclusos e inseridos no valor total a ser pago pelo CONTRATANTE;

8.1.1.3. Substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste Termo de Referência, o objeto com avarias ou defeitos;

8.1.1.4. Comunicar à Contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

8.1.1.5. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

8.1.1.6. Indicar preposto para representá-la durante a execução do contrato;

8.1.1.7. Assumir a responsabilidade pelos encargos fiscais e comerciais resultantes da adjudicação desta licitação;

8.1.1.8. Promover a destinação final ambientalmente adequada, sempre que a legislação assim o exigir;

8.1.1.9. Prestar as informações e os esclarecimentos que venham a ser solicitados pelo Município de Vitória;

8.1.1.10. A Contratada deve ser responsável por transportar seus funcionários/técnicos/profissionais, ferramentas e equipamentos, para o local de serviço e designados pelo CONTRATANTE;

8.1.1.11. Responsabilizar-se por quaisquer danos que seus funcionários/técnicos/profissionais causarem ao CONTRATANTE;

8.1.1.12. Substituir imediatamente qualquer funcionário/técnico/profissional responsável pela execução dos serviços que causar embaraço à boa execução do contrato ou por recomendação da fiscalização ou equipe técnica designada pelo CONTRANTE;

8.1.1.13. Os funcionários/técnicos/profissionais da empresa licitante contratada, preferencialmente, deverão se apresentar para a realização dos serviços trajando uniforme com logomarca da empresa e portando documento de identificação com foto;

8.1.1.14. Fornecer cabos UTP's, cabos de conexão direta (DAC) ou transceivers para "Uplinks" bem como cordões de Fibra ótica, nos switches em produção.

8.2. DA CONTRATANTE

8.2.1. São obrigações da CONTRATANTE:

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

8.2.1.2. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes deste Termo de Referência e da proposta, para fins de aceitação e recebimento definitivo;

8.2.1.3. Comunicar à CONTRATADA, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;

8.2.1.4. Acompanhar e fiscalizar o cumprimento das obrigações da CONTRATADA, através de servidor especialmente designado;

8.2.1.5. Efetuar o pagamento à CONTRATADA no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos neste Termo de Referência;

8.2.1.6. Prestar as informações e os esclarecimentos que venham a ser solicitados pelos profissionais ou técnicos da empresa licitante contratada, a ainda, para os profissionais técnicos do(s) fabricante(s) dos componentes que compõem a Solução adquirida;

8.2.1.7. Tornar disponíveis as instalações e os equipamentos necessários à prestação dos serviços, bem como, os meios necessários para o provimento para instalação e ativação da Solução adquirida, tais como: os “racks” e fornecimento de energia elétrica para alimentação dos componentes envolvidos e necessários do datacenter do CONTRATANTE, e ainda, providenciar “link de dados” e “estrutura lógica” para interconexão junto o ambiente de produção de existente.

8.2.2. 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.

CLÁUSULA NONA – DAS SANÇÕES ADMINISTRATIVAS

9.1. Ao contratado que infringir as normas constantes deste contrato ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

I. Advertência, nos casos de inexecução parcial que não acarretem prejuízos significativos para a Administração.

II. Multas nos seguintes casos e percentuais:

a) Multa de Mora: Por atraso injustificado na entrega do item contemplado na Autorização de Fornecimento (AF) / Ordem de Serviço (OS) em até 10 (dez) dias: 0,5% (cinco décimos por cento) ao dia sobre o valor da parcela descumprida;

b) Multa Compensatória: Por atraso injustificado na entrega do item contemplado na Autorização de Fornecimento (AF) / Ordem de Serviço (OS) superior a 10 (dez) dias: 10% (dez por cento) sobre o valor total do contrato, com possibilidade de cancelamento da Nota de Empenho Total ou Parcial;

c) Multa Compensatória: Por recusa injustificada do adjudicatário em aceitar ou assinar a Autorização de Fornecimento (AF) / Ordem de Serviço (OS) e/ou Contrato, injustificadamente, uma vez que caracteriza o descumprimento total da obrigação assumida: 15% (quinze por cento) sobre o valor total do contrato;

d) Multa Compensatória: Por entregar em desconformidade, injustificadamente, o objeto contemplado na Autorização de Fornecimento (AF) / Ordem de Serviço (OS): 10% (dez por cento) sobre o valor total do contrato e possibilidade de cancelamento da Nota de Empenho Total ou Parcial;

e) Multa Compensatória: Por deixar de manter as condições de habilitação durante toda a vigência contrato: 10% (dez por cento) sobre o valor total do contrato, com possibilidade de cancelamento da Nota de Empenho Total ou Parcial;

f) Multa Compensatória: Por inexecução parcial, injustificada, da Autorização de Fornecimento (AF) / Ordem de Serviço (OS): 5% (cinco por cento) sobre o valor total do contrato;

g) Multa Compensatória: Por inexecução total injustificada da Autorização de Fornecimento (AF) / Ordem de Serviço (OS). Caracterizada pela verificação da não entrega do produto/execução do serviço após 30 (trinta) dias: 15% (quinze por cento), sobre o valor total do contrato, com possibilidade de cancelamento da Nota de Empenho Total ou Parcial.

III. Impedimento de licitar e contratar com o Município de Vitória:

a) Dar causa à inexecução parcial da Autorização de Fornecimento (AF) / Ordem de Serviço (OS) e/ou do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo: até 02 (dois) anos;

b) Dar causa à inexecução total da Autorização de Fornecimento (AF) / Ordem de Serviço (OS) e/ou do contrato, caracterizada pela não entrega dos itens após 30 (trinta) dias: até 03 (três) anos;

c) Deixar de entregar a documentação exigida para o certame: até 02 (dois) anos;

d) Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado: até 03 (três) anos;

e) Não celebrar o contrato/instrumento congênere ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta: até 03 (três) anos;

f) Ensejar o retardamento da entrega do objeto da licitação sem motivo justificado, superior a 20 (dez) dias: até 03 (três) anos.

IV. Declaração de inidoneidade para licitar ou contratar com a Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos seguintes casos:

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

b) Fraudar a licitação ou praticar ato fraudulento na execução do contrato;

c) Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

d) Praticar atos ilícitos com vistas a frustrar os objetivos da licitação; e,

e) Praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

9.2. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo específico que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário/contratado, observando-se o procedimento previsto na Lei nº 14.133/2021.

9.3. Os atos previstos como infrações administrativas na Lei nº 14.133/2021 ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846/2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e a autoridade competente definidos no Decreto Municipal nº 16.522/2015.

9.4. A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública, previstas na Lei nº 12.846/2016 seguirão seu rito previsto na Lei nº 14.133/2021.

9.5. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor de pagamento eventualmente devido pela Administração ao contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

9.6. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade poderão ser aplicadas cumulativamente com a sanção de multa.

9.7. Na aplicação das sanções, serão considerados a natureza e a gravidade da infração cometida, as peculiaridades do caso concreto, as circunstâncias agravantes ou atenuantes, os danos que dela provierem para a Administração Pública, e a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

CLÁUSULA DÉCIMA – DA SUBCONTRATAÇÃO

10.1. É permitida a subcontratação parcial do objeto, até o limite de 30 % (trinta por cento) do valor total contratado.

10.2. É vedada a sub-rogação completa ou da parcela principal da obrigação.

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

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

10.5. Não serão realizados pagamentos diretamente à subcontratadas.

10.6. A subcontratação será formalizada de acordo com o seguinte procedimento:

10.6.1. Submissão, pela CONTRATADA, de pedido fundamentado de que subcontratação, acompanhado de planilha detalhada demonstrando a quantidade e o valor das parcelas que serão subcontratadas;

10.6.2. Autorização prévia, por escrito, da CONTRATANTE para a subcontratação;

10.6.3. Apresentação de cópia do Termo de Subcontratação ou ajuste equivalente celebrado entre a contratada e subcontratada, o qual será juntado aos autos do processo administrativo.

10.7. Somente serão permitidas as subcontratações prévias e regularmente autorizadas pela CONTRATANTE. A subcontratação não formalizada segundo o procedimento previsto no edital, constituirá motivo para a rescisão unilateral do contrato.

10.8. 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 licitação 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.

CLÁUSULA DÉCIMA PRIMEIRA – DAS SUPRESSÕES OU ACRÉSCIMOS

11.1. A Contratada obrigar-se-á a aceitar, nas mesmas condições estabelecidas na Autorização de Fornecimento (AF) / Ordem de Serviços (OS) e/ou Contrato, os acréscimos e supressões que se fizerem necessários, em até 25% (vinte e cinco por cento) do valor inicial atualizado.

CLÁUSULA DÉCIMA SEGUNDA - DO REEQUILÍBRIO ECONÔMICO-FINANCEIRO

12.1. A recomposição do equilíbrio econômico-financeiro do contrato, além de obedecer aos requisitos previstos no artigo 124, inciso II, "d", da Lei Federal nº 14.133/2021, será proporcional ao desequilíbrio efetivamente suportado, cuja existência e extensão deverão ser comprovados pela CONTRATADA ou pelo CONTRATANTE, conforme o caso, e darão ensejo à alteração do valor do contrato para mais ou para menos, respectivamente.

12.2. O reequilíbrio econômico-financeiro não possui data-base para ocorrer, não exige a fluência de prazo mínimo de transcurso contratual e nem pode retroagir, senão, até o mês da data do protocolo do respectivo pedido.

12.3. A resposta ao pedido de restabelecimento do equilíbrio econômico-financeiro, quando ocorrer, será concedida no prazo máximo de 01 (um) mês.

CLÁUSULA DÉCIMA TERCEIRA – DO REAJUSTAMENTO

13.1. Os preços serão fixos e irreajustáveis pelo período de 12 (doze) meses, a partir de quando poderá ser concedido reajuste, a contar da data do orçamento, com base no índice ICTI-IPEA ou outro índice que vier a substituí-lo, desde que devidamente comprovado e aceito pela Administração.

13.2. A resposta ao pedido de reajustamento, quando ocorrer, será concedida no prazo máximo de 01 (um) mês.

CLÁUSULA DÉCIMA QUARTA – DA GARANTIA

14.1. A CONTRATADA fica obrigada a apresentar garantia contratual, em valor correspondente a 5% (cinco por cento) do valor anual do contrato.

14.2. Caberá a CONTRATADA optar por uma das seguintes modalidades de garantia:

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

II. Seguro-garantia;

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

14.3. A garantia nas modalidades caução e fiança bancária deverá ser prestada em até 15 (quinze) dias após a assinatura do contrato.

14.4. O seguro-garantia deverá ser apresentado, no máximo, até a data de assinatura do contrato.

14.5. Na hipótese de suspensão do contrato por ordem ou inadimplemento da Administração, a CONTRATADA ficará desobrigado de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pela Administração.

14.6. O prazo de vigência da apólice será igual ou superior ao prazo estabelecido no contrato principal e deverá acompanhar as modificações referentes à vigência deste mediante a emissão do respectivo endosso pela seguradora;

14.7. O seguro-garantia continuará em vigor mesmo se a CONTRATADA não tiver pago o prêmio nas datas convencionadas.

14.8. A garantia prestada pela CONTRATADA será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da Administração e, quando em dinheiro, atualizada monetariamente.

14.9. Em se tratando de fiança bancária, títulos da dívida pública ou seguro-garantia, o documento pertinente deverá ser apresentado ao Gestor do Contrato, que se encarregará de confirmar a autenticidade do documento, anexar cópia do mesmo no processo de formalização do contrato, bem como encaminhar a via original à SEMFA/GPC/CCASP para registro no sistema de contabilidade.

14.10. O título da dívida pública a ser ofertado tem que ser um título atual, em circulação normal no mercado, e com possibilidade de resgate imediato.

14.11. Quando se tratar de caução em dinheiro, a mesma deverá ser recolhida pela licitante vencedora através do DUA - Documento Único de Arrecadação no Código dos Tributos - Outras Receitas Correntes nº 4610.

14.12. O depósito da caução em dinheiro, deverá ser efetuado na(s) conta(s) específica(s) do Contratante, conforme descrito abaixo:

[Inserir conta(s) bancária(s) do(s) órgão(s) requisitante(s)]

14.13. Havendo prorrogação do prazo formalmente admitida pela Administração, deverá a CONTRATADA reapresentar quaisquer das modalidades de garantia previstas neste Contrato e por essa escolhida, de forma a abranger o período de prorrogação, retendo a CONTRATANTE dos créditos da contratada, enquanto não efetivar tal garantia, o valor a ela correspondente.

14.14. Ocorrendo aumento no valor contratual por acréscimo, respeitando o limite de 25% (vinte e cinco por cento) a Contratada deverá proceder o reforço da garantia inicial no mesmo percentual estabelecido nesta cláusula.

CLÁUSULA DÉCIMA QUINTA – DA RESCISÃO

15.1. Este contrato poderá ser rescindido pelo CONTRATANTE, independentemente de notificação ou interpelação judicial, atendido o disposto nos arts. 137 a 139 da Lei nº 14.133/2021.

CLÁUSULA DÉCIMA SEXTA - DOS CASOS OMISSOS

16.1. Os casos omissos serão decididos pela Contratante, segundo as disposições contidas na Lei nº 14.133/2021 e demais normas aplicáveis a matéria e princípios gerais dos contratos.

CLÁUSULA DÉCIMA SETIMA – DO FORO

17.1. Fica eleito o Foro da Vara dos Feitos da Fazenda Pública Municipal, Comarca da Capital, Vitória, ES, para dirimir quaisquer dúvidas oriundas do presente contrato.

E assim, por estarem justos e acordados, assinam o presente instrumento em 02 (duas) vias de igual teor e forma (assinatura física) e, no caso de utilização de assinatura digital qualificada, será em somente 01 (uma) via, para que surta um só efeito e a data do termo deverá ser considerada a data da última assinatura.

Vitória, XX de XXXXXXXXX de XXXX.

XXXXXXXXXXXXXXXXXXX

SECRETÁRIO MUNICIPAL DE XXXXXXXXXXXXXXX

CONTRATANTE

XXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXX

CONTRATADA

TESTEMUNHAS:

1) _____

2) _____