



ESTADO DO ACRE
SECRETARIA DE ESTADO DA FAZENDA

Rua Benjamin Constant, 946, - Bairro Centro, Rio Branco/AC, CEP 69900-062
- <http://www.sefaz.ac.gov.br/>

TERMO DE REFERÊNCIA Nº 62/2025/SEFAZ - DIPROJ

Processo nº 0715.007435.00044/2025-61

1. SUMÁRIO

[APRESENTAÇÃO](#)

[DO OBJETO DA CONTRATAÇÃO](#)

[DA JUSTIFICATIVAS DA NECESSIDADE DA CONTRATAÇÃO](#)

[DAS ESPECIFICAÇÕES TÉCNICAS MÍNIMAS](#)

[DA NATUREZA DA CONTRATAÇÃO E ALINHAMENTO ESTRATÉGICO](#)

[DA FUNDAMENTAÇÃO DA CONTRATAÇÃO](#)

[DO PARCELAMENTO DO OBJETO](#)

[OUTROS REQUISITOS DA CONTRATAÇÃO](#)

[DO PRAZO DA CONTRATAÇÃO](#)

[DO MODELO DE EXECUÇÃO DO OBJETO](#)

[DAS OBRIGAÇÕES DA CONTRATANTE](#)

[DAS OBRIGAÇÕES DA CONTRATADA](#)

[DO MODELO DE GESTÃO DO CONTRATO](#)

[CRITÉRIOS DE PAGAMENTO E PREÇO](#)

[DA FORMA DE SELEÇÃO DO FORNECEDOR](#)

[DA PARTICIPAÇÃO DE CONSÓRCIOS](#)

[ATA DE REGISTRO DE PREÇOS](#)

[DA ADEQUAÇÃO ORÇAMENTÁRIA](#)

[ANEXOS](#)

[RESPONSABILIDADES](#)

2. APRESENTAÇÃO

2.1. O objeto desta contratação possui características comuns e padronizadas pelo mercado, sendo a descrição e os padrões de desempenho e qualidade possíveis de definir no Edital e no Termo de Referência, de maneira objetiva e suficientemente exaustiva e clara, a ponto de não suscitar dúvidas acerca das especificações do objeto pretendido, sendo caracterizado com bens e serviços comuns e de natureza contínua, conforme previsto no inciso XIII e XV do art. 6º da Lei nº 14.133/2021.

3. DO OBJETO DA CONTRATAÇÃO

3.1. **Objeto**

3.1.1. Contratação de empresa especializada para prestação de serviços continuados de links de acesso a internet dedicados, serviços de proteção contra ataques DDoS e solução de proteção de perímetro gerenciado, com alta disponibilidade de hardware (cluster), visando atender às necessidades de conectividade da SEFAZ/AC, conforme descrito na tabela abaixo e de acordo com as descrições e quantidades estabelecidas neste Termo de Referência.

3.1.2. **Tabela.** Descrição e Quantidades:

LOTE 1							
ITEM (a)	DESCRIÇÃO (b)	VELOCIDADE (c)	UNID. (d)	QUANT. REGISTRO (e)	VALOR UNITÁRIO (f)	VALOR DO ITEM EM 60 MESES (g)	VALOR TOTAL (h) = (e) x (g)
1	Serviço de Link dedicado de acesso a internet - (Principal)	5 Gbps	Unid.	2	33.647,06	2.018.823,45	4.037.646,90
2	Serviço de mitigação de ataques de negação de serviço - DDOS	-	Unid.	2	10.287,50	617.250,15	1.234.500,30
Valor Total Lote 1						2.636.073,60	5.272.147,20
LOTE 2							
2	Serviço de Link dedicado de acesso a internet - (Redundância)	5 Gbps	Unid.	2	33.647,06	2.018.823,45	4.037.646,90
2	Serviço de mitigação de ataques de negação de serviço - DDOS	-	Unid.	2	10.287,50	617.250,15	1.234.500,30
Valor Total Lote 2						2.636.073,60	5.272.147,20
LOTE 3							
2	Solução de Segurança de Perímetro	-	Unid.	2	28.091,67	1.685.500,20	3.371.000,40
2	WAF - Web Application Firewall	-	Unid.	2	29.345,19	1.760.706,00	3.521.412,00
Valor Total Lote 3						3.446.296,20	6.892.412,40
Valor Total							17.436.706,80

3.1.3. Nos preços propostos deverão estar inclusos todos os custos fixos ou variáveis, necessários à perfeita execução do Contrato (custos diretos e indiretos, inclusive os resultantes da incidência de quaisquer impostos, taxas, contribuições ou obrigações trabalhistas, fiscais, previdenciárias, transportes, seguros, embalagens, deslocamento de pessoal, alimentação etc.).

3.2. Os itens que compõem o objeto serão adjudicados de forma lotes. Tal exigência justifica-se pela integração das atividades necessária para a execução do projeto.

4. DA JUSTIFICATIVAS DA NECESSIDADE DA CONTRATAÇÃO

4.1. Contextualização

4.1.1. A Secretaria de Estado da Fazenda do Acre (SEFAZ/AC) é responsável pela gestão da arrecadação tributária estadual e pela manutenção de diversos sistemas corporativos que operam de forma contínua e ininterrupta. Esses sistemas suportam o funcionamento da máquina pública e a prestação de serviços digitais ao contribuinte, sendo essenciais para o cumprimento da missão institucional do órgão. O desempenho adequado desses serviços depende diretamente da disponibilidade de uma infraestrutura de conectividade robusta, segura e com alta capacidade de resposta.

Atualmente, a SEFAZ/AC mantém o Contrato nº 34/2021 com a empresa OI S.A., cujo objeto é a prestação de serviços continuados de acesso dedicado à internet com velocidade de 300 Mbps. Através do 5º Termo Aditivo, ocorreu o Upgrade de velocidade do link de acesso à Internet de 300 Mbps (Mega bits por segundo) para 1 Gbps (Giga bits por segundo), incluindo proteção contra ataques DDoS e solução de segurança perimetral gerenciada com alta disponibilidade (cluster). Cujo o mesmo foi celebrado inicialmente por 12 meses, o contrato possui vigência prorrogável até 2 de dezembro de 2026, conforme previsto na Lei nº 8.666/1993.

4.1.2. Apesar das melhorias implementadas, a solução contratada passou a apresentar sinais de saturação frente ao aumento exponencial das atividades digitais da instituição. O crescimento do volume de dados trafegados, a ampliação dos serviços online ofertados ao contribuinte e o uso intensivo de aplicações em nuvem exigem uma infraestrutura de conectividade ainda mais robusta e escalável. Essa realidade impõe a necessidade de reavaliação da atual solução, visando garantir a continuidade, a segurança e a performance dos serviços prestados.

4.2. Descrição do Problema

4.2.1. O problema identificado refere-se ao aumento progressivo das demandas institucionais da Secretaria de Estado da Fazenda do Acre (SEFAZ/AC), decorrente da operação de sistemas essenciais como emissão de documentos fiscais eletrônicos (NF-e, NFC-e, CT-e, MDF-e), escrituração digital (EFD, GIA-ST), sincronização com bases nacionais, serviços de correio eletrônico institucional e acesso a plataformas em nuvem. Diante desse cenário, a largura de banda atualmente contratada revelou-se insuficiente, ocasionando gargalos de rede, instabilidade, lentidão e risco de indisponibilidade dos serviços prestados à sociedade e aos contribuintes.

4.2.2. Adicionalmente, o crescimento no uso de videoconferências, sistemas remotos e aplicações digitais intensificou o volume de tráfego de dados, pressionando ainda mais a infraestrutura existente. A ausência de um link redundante e de soluções modernas de segurança eleva significativamente o risco de falhas operacionais, interrupções de serviço e vulnerabilidades no ambiente tecnológico da SEFAZ/AC, comprometendo a continuidade das atividades administrativas e finalísticas do órgão.

4.3. Motivação da demanda

4.3.1. A nova contratação mostra-se necessária uma vez que, apesar da vigência do contrato atual, a infraestrutura contratada não acompanhará a evolução das necessidades institucionais nos próximos anos. A velocidade de conexão em vigor poderá tornar-se insuficiente frente ao crescimento contínuo das atividades digitais, o que resultaria em picos recorrentes de consumo de banda, falhas de acesso e indisponibilidades em sistemas essenciais à administração tributária.

4.3.2. O avanço tecnológico e a digitalização dos serviços públicos exigem uma infraestrutura de conectividade moderna, com alta capacidade de resposta e soluções de segurança atualizadas, capazes de mitigar riscos cibernéticos. O modelo vigente, embora eficaz à época de sua contratação, já não contempla a complexidade atual dos serviços prestados pela SEFAZ/AC. Assim, é imprescindível a contratação de nova solução tecnológica, aderente às boas práticas de governança em tecnologia da informação e às diretrizes da Administração Pública.

4.4. Benefícios e Resultados Esperados:

- a) **Ampliação da capacidade de banda para 5 Gbps**, garantindo desempenho compatível com as atuais e futuras necessidades de tráfego de dados;
- b) **Implantação de redundância de link**, assegurando a continuidade dos serviços mesmo em caso de falha ou indisponibilidade do link principal;
- c) **Eliminação de gargalos de rede**, promovendo maior estabilidade e fluidez nos serviços digitais;
- d) **Proteção robusta contra ataques DDoS**, mitigando riscos de indisponibilidade provocados por ameaças externas;
- e) **Segurança perimetral gerenciada**, com tecnologia atualizada e respostas proativas a incidentes de segurança;

f) **Melhoria no atendimento ao contribuinte**, com maior estabilidade e agilidade nos sistemas públicos;

g) **Prevenção de riscos operacionais**, decorrentes de falhas de conectividade ou limitações tecnológicas da infraestrutura atual.

4.5. Da Natureza da Prestação dos Serviços

4.5.1. A prestação de serviços é de natureza continuada em razão de sua essencialidade para a Instituição, uma vez que as soluções tecnológicas envolvidas são de missão crítica e não podem sofrer descontinuidade, pois colocariam em risco o funcionamento e integridade das atividades da Administração Pública. Neste sentido se pronunciou o TCU:

“(…)o que caracteriza o caráter contínuo de um determinado serviço é sua essencialidade para assegurar a integridade do patrimônio público de forma rotineira e permanente ou para manter o funcionamento das atividades finalísticas do ente administrativo, de modo que sua interrupção possa comprometer a prestação de um serviço público ou o cumprimento da missão institucional.” (TCU. Acórdão nº 132/2008 – Segunda Câmara. Relator: Ministro Aroldo Cedraz).

5. DA DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

5.1. Para atender de forma integrada e resiliente às crescentes demandas de conectividade, desempenho e segurança da Secretaria de Estado da Fazenda do Acre (SEFAZ/AC), propõe-se uma solução estruturada em três lotes complementares. Cada lote foi concebido para garantir não apenas a capacidade de tráfego necessária às operações críticas, que incluem emissão de documentos fiscais eletrônicos, escrituração digital e plataformas de comunicação remota, mas também para oferecer camadas de proteção automatizadas contra ataques cibernéticos e mecanismos de redundância que asseguram a continuidade dos serviços em qualquer cenário.

5.2. Divisão de lotes

5.2.1. A proposta alinha-se aos princípios de eficiência, economicidade e legalidade da administração pública, centralizando a gestão contratual e técnica, sendo:

a) **Link Primário com Mitigação DDoS** - Um **enlace dedicado simétrico de 5 Gbps**, dimensionado para suportar todos os sistemas críticos da Secretaria (emissão de NF-e, escrituração digital, videoconferência, etc.), com **SLA de alta disponibilidade**. A mitigação de ataques de negação de serviço (DDoS) é nativa ao contrato do link, atuando automaticamente nas camadas de rede (L3/L4) para proteger contra surtos de tráfego malicioso, sem necessidade de ações manuais ou integrações externas.

b) **Link de Redundância com Mitigação DDoS** - Um **segundo enlace dedicado simétrico de 5 Gbps**, configurado em redundância ativa/passiva via BGP, assegurando failover instantâneo em caso de falha do link primário. Também inclui o mesmo nível de **proteção DDoS integrada**, garantindo que tanto o canal principal quanto o de contingência mantenham resiliência contra ataques volumétricos.

c) **Segurança Perimetral em Alta Disponibilidade com WAF Virtualizado** - Appliance de **firewall físico dedicado**, entregue em configuração de **cluster HA (ativo/ativo ou ativo/passivo)**, instalado no datacenter da SEFAZ/AC. O equipamento oferece **inspeção profunda de pacotes (DPI), IPS/IDS, controle de aplicações, filtragem de conteúdo e SSL Inspection**, garantindo o bloqueio de ameaças avançadas e a manutenção da integridade do perímetro de rede.

5.3. Instalação e Aceite

5.3.1. Para todos os itens contratados, a instalação será executada em junto com a equipe técnica da SEFAZ/AC e abrangerá as seguintes etapas:

a) **Planejamento Detalhado:** Definição conjunta do cronograma, identificação das janelas de intervenção e análise de riscos, para minimizar qualquer impacto às operações diárias da Secretaria.

b) **Adaptações Cíveis e Elétricas:** Realização de obras de passagem de cabos, instalações de suportes e ajustes na infraestrutura elétrica, com posterior recomposição do ambiente à sua condição original.

c) **Configuração e Testes de Desempenho:** Parametrização de todos os componentes da solução (enlaces, dispositivos de segurança e dispositivos de redundância) e execução de testes de velocidade, latência, failover e conformidade técnica.

d) **Validação e Aceite Formal:** Emissão de relatórios de testes em duas vias, a serem assinados pela equipe da SEFAZ/AC, condicionando o início da faturação ao aceite oficial, garantindo que o serviço instalado atenda a todos os requisitos contratuais.

5.4. Recomendação Técnica

5.4.1. Com base na análise das necessidades operacionais da Secretaria de Estado da Fazenda do Acre (SEFAZ/AC), recomenda-se tecnicamente a adoção de uma solução composta por link dedicado simétrico de alta capacidade, proteção contra ataques DDoS integrada ao link e firewall perimetral físico em alta disponibilidade integrado com o WAF Virtualizado (On-Premise). Essa combinação atende aos requisitos de desempenho, segurança e confiabilidade exigidos para o funcionamento ininterrupto dos sistemas fiscais e corporativos da instituição, garantindo comunicação estável com órgãos federais, serviços em nuvem e contribuintes.

5.4.2. A opção pelo link dedicado simétrico assegura banda garantida com desempenho equilibrado entre download e upload, o que é essencial para os serviços que operam 24/7, como emissão de documentos fiscais eletrônicos, escrituração digital e sincronização de dados. A proteção DDoS integrada ao link simplifica a gestão contratual e operacional, oferecendo mitigação automatizada diretamente pela operadora, com resposta imediata a incidentes e sem a necessidade de integração com plataformas terceiras.

5.4.3. Por fim, o firewall perimetral físico com WAF Virtualizado, instalado em cluster no datacenter da SEFAZ/AC, permite controle total sobre a segurança da rede, oferecendo alta capacidade de inspeção, redundância e personalização das políticas de segurança. Essa arquitetura garante maior robustez frente a ameaças, continuidade dos serviços críticos e conformidade com os princípios da administração pública, sendo, portanto, a alternativa mais segura e eficiente do ponto de vista técnico e institucional.

5.5. Justificativa Técnica

5.5.1. A escolha da solução de segurança perimetral e proteção de aplicações web da fabricante **FORTINET**, com os modelos **FG-401F** (firewall) e **FortiWEB** (WAF), fundamenta-se no **princípio da padronização**, expressamente previsto na **Lei nº 14.133/2021**, que orienta a Administração Pública a uniformizar soluções técnicas visando **compatibilidade, eficiência operacional e economicidade**.

5.5.2. Conforme dispõe o **art. 40, inciso V, alínea “a”** da referida lei:

“Art. 40 O planejamento de compras deverá considerar a expectativa de consumo anual e observar o seguinte:

(...)

V – atendimento aos princípios:

a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenhos;

5.5.3. Nesse sentido, a padronização da arquitetura Fortinet se justifica tecnicamente, pois a SEFAZ/AC já opera com equipamentos **FortiGate 40F** em sua rede WAN corporativa (MPLS), conforme previsto no **Contrato nº 25/2023**, vigente e com prorrogação prevista. Essa infraestrutura interliga as agências, postos fiscais e a sede da instituição, e exige **plena interoperabilidade e gerenciamento centralizado** com o firewall de borda e a solução de WAF.

5.5.4. A substituição do modelo atualmente utilizado, **FG-601E** (objeto do **Contrato nº 34/2021** com a empresa OI S.A.), pelo modelo **FG-401F**, da mesma fabricante, garante **continuidade operacional, compatibilidade nativa, atualização tecnológica e evolução de desempenho**, com total integração à estrutura existente — evitando retrabalho, riscos de incompatibilidade e custos adicionais com treinamento ou suporte técnico.

5.5.5. O **art. 41, inciso I, alíneas “a” e “b”**, reforça a legalidade da escolha padronizada ao dispor:

“Art. 41 No caso de licitação que envolva o fornecimento de bens, a Administração poderá excepcionalmente:

I – indicar uma ou mais marcas ou modelos, desde que formalmente justificado, nas seguintes hipóteses:

a) em decorrência da necessidade de padronização do objeto;

b) em decorrência da necessidade de manter a compatibilidade com plataformas e padrões já adotados pela Administração;

(...)

5.5.6. Portanto, a escolha por manter a plataforma Fortinet assegura **uniformidade tecnológica, integração direta entre os dispositivos da rede**, e um ambiente de segurança consolidado, cujo suporte já é dominado pela equipe técnica interna. Além disso, evita-se a adoção de soluções heterogêneas que poderiam gerar conflitos de configuração, falhas de interoperabilidade e aumento de custos operacionais.

5.5.7. Por fim, destaca-se o **art. 47, inciso I**, que trata das licitações de serviços, também reforça a adoção da padronização:

“Art. 47 As licitações de serviços atenderão aos princípios:

I – da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;

(...)

5.5.8. Dessa forma, a padronização com os modelos FG-401F e FortiWEB se justifica pelos seguintes fatores técnicos e operacionais:

a) **Compatibilidade e integração com a infraestrutura atual** da SEFAZ/AC, que já opera com equipamentos FortiGate 40F, contratados por meio do **Contrato nº 25/2023**, cuja vigência está assegurada e cuja prorrogação é prevista para atender às necessidades crescentes da rede WAN corporativa (MPLS) que interliga todas as agências e postos fiscais.

b) **Interoperabilidade nativa** entre os equipamentos Fortinet, permitindo gerenciamento centralizado, políticas de segurança unificadas e comunicação direta entre o firewall perimetral (FG-401F), os equipamentos nas agências (FortiGate 40F) e a solução de WAF (FortiWEB), sem necessidade de integrações complexas, que aumentariam custos e riscos.

c) **Redução de riscos operacionais**, uma vez que a adoção de equipamentos de fabricantes distintos poderia gerar incompatibilidades, dificultar o suporte, aumentar o tempo de resposta a incidentes e comprometer a segurança da rede e dos sistemas.

d) **Ganhos de escala e racionalização de custos de suporte técnico, manutenção e capacitação**, considerando que a equipe técnica da SEFAZ/AC já possui conhecimento na linha Fortinet, o que elimina a necessidade de treinamento adicional e acelera a implantação da nova solução.

e) **Alinhamento à solução atualmente em operação**, que utiliza o modelo **FG-601E**, fornecido no âmbito do **Contrato nº 34/2021** com a empresa OI S.A. A substituição pelo modelo FG-401F, mais atual, garante a continuidade operacional e atualização tecnológica dentro da mesma plataforma, com ganho de desempenho e recursos avançados de segurança.

f) **Atendimento a requisitos modernos de segurança da informação**, como proteção contra ataques DDoS, inspeção de tráfego criptografado (SSL Inspection), filtragem de conteúdo, prevenção contra intrusão (IPS), e especialmente, **proteção de aplicações web com uso da FortiWEB**, que assegura camada adicional de defesa contra ataques direcionados a sistemas acessíveis via internet (como páginas de emissão de NF-e, consulta de débitos, webmail, etc.).

5.5.9. A continuidade da plataforma **Fortinet**, já adotada institucionalmente pela SEFAZ/AC, promove a **inovação tecnológica** por meio da incorporação de equipamentos mais modernos e eficientes, ao mesmo tempo em que proporciona **redução de custos com licenciamento, suporte, manutenção e integração**. Essa escolha representa a **melhor relação custo-benefício** para a Administração Pública, pois evita a necessidade de reestruturação da infraestrutura tecnológica já consolidada. Assim, a manutenção da arquitetura Fortinet configura-se como uma **medida técnica necessária, estratégica e proporcional**, alinhada aos princípios da **padronização, eficiência, economicidade e segurança da informação**, assegurando a continuidade operacional, a interoperabilidade entre os sistemas e a evolução segura da infraestrutura de TIC da SEFAZ/AC.

5.5.10. Conclusão

5.5.10.1. Para maximizar a **resiliência** e assegurar **verdadeira redundância**, a contratação do **Link Primário (Lote I)** e do **Link de Contingência (Lote II)** deverá ocorrer junto a **fornecedores distintos**, evitando qualquer ponto único de falha. Dessa forma, cada enlace desenvolverá sua função de forma independente, garantindo failover efetivo e continuidade ininterrupta dos serviços críticos da SEFAZ/AC.

5.5.10.2. O **Lote III – Segurança Perimetral em Alta Disponibilidade** seguirá a **padronização dos equipamentos já implantados** no datacenter da SEFAZ/AC, mantendo coerência operacional e facilitando a **gestão unificada de políticas de segurança**, firmware e licenciamento. Essa uniformidade assegura compatibilidade total com as rotinas de manutenção, monitoramento e escalonamento de suporte técnico.

5.5.10.3. Ao centralizar a supervisão contratual e técnica nesses três lotes, a SEFAZ/AC promove ganhos significativos em **eficiência administrativa, economicidade e transparência**. O modelo reduz burocracias, simplifica a fiscalização e reforça a responsabilidade de cada prestadora pelos seus respectivos serviços.

5.5.10.4. A implantação, conduzida de forma colaborativa com a equipe técnica da SEFAZ/AC e submetida a **rigorosos testes de desempenho, failover e validação formal**, assegurará a conformidade de cada componente com os padrões contratuais. Essa abordagem integrada viabiliza uma infraestrutura de conectividade moderna, segura e

sem pontos únicos de falha, capaz de sustentar a evolução dos serviços digitais públicos e proteger eficazmente contra ameaças cibernéticas.

6. DAS ESPECIFICAÇÕES TÉCNICAS MÍNIMAS

6.1. Condições Gerais para os Lotes I e II

6.1.1. A vencedora do LOTE 01, não poderá ser a vencedora do LOTE 02 e vice-versa. Objetivando atender aos requisitos de saídas distintas de conectividade para promover a redundância do serviço;

6.1.2. As empresas vencedoras do LOTE 01 e LOTE 02 não poderão compartilhar backbone entre si, dadas as necessidades de redundância apresentadas pela SEFAZ/AC;

6.1.3. Os links de acesso à Internet fornecidos por uma empresa vencedora deverão possuir rotas físicas completamente distintas e independentes, de ponta a ponta, da outra empresa vencedora, garantindo que não existam pontos únicos de falha.

6.2. LOTE I

6.2.1. Link dedicado de acesso a internet (Principal)

6.2.1.1. REQUISITOS MÍNIMOS

- a) O link deverá ser provido no datacenter da SEFAZ/AC, na velocidade mínima de 5 Gbps.
- b) A CONTRATADA deverá fornecer junto ao Link Dedicado de 5 Gbps, endereços IPv4 válidos com pelo menos uma sub-rede /26, sendo 64 endereços IP válidos na internet;
- c) Os endereços IP deverão ser reservados pela CONTRATADA exclusivamente para a CONTRATANTE, independente de utilização;
- d) Deverá ser disponibilizado acesso permanente que possibilite a interligação do ambiente da CONTRATANTE à rede mundial de computadores, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, composto de um canal direto com a Internet de uso ilimitado, em conformidade com os prazos definidos no Acordo de Nível de Serviço;
- e) O acesso não poderá ser compartilhado com nenhum outro cliente da CONTRATADA e deverá ser capaz de absorver 100% (cem por cento) do tráfego referente à velocidade contratada;
- f) O backbone ofertado deverá possuir, a partir da cidade de Rio Branco/AC, no mínimo duas abordagens físicas e lógicas distintas própria ou de terceiros, desde comprovada que a largura de banda atenda o dobro da solicitação da SEFAZ, garantindo rotas redundantes para a saída de tráfego nacional e internacional, de modo a assegurar a alta disponibilidade e a continuidade do serviço.
- g) A CONTRATADA deverá possuir saída de backbone internacional com capacidade de transmissão de pelo menos 10 Gbps;
- h) Todo fornecimento e instalação dos materiais e equipamentos necessários à prestação dos serviços pela CONTRATADA, não poderá acarretar ônus adicional à CONTRATANTE, logo, deverão estar inclusos na solução todos os recursos de conectividade, tais como: modems, conversores, roteadores, e outros correlatos necessários à prestação dos serviços, exceto racks e tomadas de energia;
- i) Os equipamentos fornecidos deverão ser capazes de atender INTEGRALMENTE aos requisitos de qualidade e velocidade do link de comunicação de dados contratado;
- j) Os roteadores integrantes do backbone da prestadora de serviços e os roteadores instalados no datacenter da CONTRATANTE deverão possuir capacidade de suportar o tráfego com banda completamente ocupada, sem que os limites de 70% de utilização da CPU sejam excedidos;
- k) Os recursos de hardware e software dos equipamentos devem ser atualizados tecnologicamente, sem ônus para a CONTRATANTE, durante a vigência do contrato;
- l) Os equipamentos fornecidos deverão permitir a instalação em rack de 19 polegadas, devendo vir acompanhado de todas as peças e acessórios necessários para fixação;
- m) Os equipamentos fornecidos deverão possuir fonte de alimentação redundante com entrada 110/220 volts AC e com a frequência de 60 Hz, com comutação automática de tensão;
- n) Os equipamentos fornecidos deverão acompanhar todos os acessórios necessários para operacionalização do equipamento (softwares, sistemas operacionais, cabos lógicos de

gerenciamento/console, cabos de energia elétrica seguindo o novo padrão brasileiro de tomadas);

o) O equipamento de entrega de última milha deve possuir pelo menos 2 (duas) interfaces 10 Gigabit Ethernet com conector SFP+ e transceiver compatível com o equipamento instalado na SEFAZ/AC para entrada de links (FORTIGATE 401F) e 1 (uma) interface Gigabit Ethernet com conector RJ-45. Todos os cabos necessários para conexão entre os equipamentos serão de responsabilidade da CONTRATADA;

p) Sempre que houver lançamento de nova versão estável de sistema operacional e ou firmware que faça correções de segurança dos equipamentos fornecidos, a CONTRATADA deverá providenciar as atualizações com prévia aprovação da CONTRATANTE, sem ônus adicional;

q) O link e equipamentos fornecidos pela CONTRATADA, nas suas condições de fabricação, operação, manutenção, configuração, funcionamento, alimentação e instalação, deverão obedecer rigorosamente às normas e recomendações em vigor, elaboradas por órgãos oficiais competentes ou entidades autônomas reconhecidas na área – ABNT (Associação Brasileira de Normas Técnicas) e ANATEL (Agência Nacional de Telecomunicações), e entidades de padrões reconhecidas internacionalmente – ITU-T (Internacional Telecommunication Union), ISO (International Standardization Organization), IEEE (Institute of Electrical and Electronics Engineers), EIA/TIA (Electronics Industry Alliance and Telecommunication Industry Association);

r) A CONTRATADA deverá fornecer as senhas de acesso, via porta de console e via SSHv2, para cada um dos roteadores instalados, com privilégios somente para operações de leitura – (read only) para os comandos “ping”, “tracert” e “trace”. Também deverá ser fornecido acesso somente de leitura às estatísticas de SNMP (comunidade de leitura ou usuário/senha), além de configurar os roteadores para gerar logs (Syslog – RFC 3164) e/ou traps SNMP para um ou mais endereços IPs a serem definidos pela CONTRATANTE;

s) Todo conjunto de materiais e equipamentos fornecidos pela CONTRATADA, deverão ser novos e sem uso prévio, atendendo as normas do Código de Defesa do Consumidor, não podendo ser reciclados ou recondicionados e nem de fabricação artesanal;

t) Deverá dispor de reserva técnica de componentes sobressalentes suficientes, caso haja necessidade de substituição;

u) Todo e qualquer equipamento, acessório ou interface, ainda que não mencionados neste documento, porém, necessário à composição da solução ou necessário ao atendimento de qualquer funcionalidade ou configuração requerida neste documento deverá estar incluída na solução proposta, sem implicação de ônus adicional para a CONTRATANTE;

v) Os equipamentos que se mostrarem necessários deverão ser fornecidos pela CONTRATADA, em regime de comodato;

6.2.1.2. ESCALABILIDADE

a) Ajuste Dinâmico de Largura de Banda: A infraestrutura de um link dedicado permite ajustes dinâmicos na largura de banda, permitindo escalabilidade conforme as necessidades de crescimento da empresa;

b) O circuito deverá permitir aumento de velocidade e troca de rotas, de acordo com a demanda futura da SEFAZ, o que poderá ser objeto de aditivo contratual, nos termos e limites legais;

c) O tempo máximo para alteração da velocidade de acesso deverá ser de 05 (cinco) dias úteis após a assinatura do correspondente termo aditivo ao contrato;

d) No caso de aumento da velocidade do link de comunicação (upgrade), será permitida a substituição do equipamento/roteador e/ou interface de conexão para que o serviço continue sendo prestado em conformidade com o previsto neste Termo.

6.2.1.3. PENALIDADES

a) As penalidades abaixo serão aplicadas sobre os valores individuais de cada acesso analisado e constarão na fatura mensal do período subsequente ao da(s) ocorrência(s). No caso de descumprimento, pela CONTRATADA, de mais de um Nível de Serviço acordado, num mesmo período, num determinado acesso, as penalidades serão somadas até o valor máximo de 100% (cem por cento):

- Taxa de erros média mensal (mínimo de dez amostras, em dias distintos) maior que a contratada:

10%

- Prazo de instalação ou de mudança de endereço de instalação ou de mudança de velocidade maior que o contratado: 10% + 0,5% por dia inteiro de atraso;
- Prazo para recuperação/reparação do serviço maior que o contratado: 10% + 1% por hora inteira de atraso;
- Nota: As penalidades poderão ser reduzidas ou anuladas caso a CONTRATADA justifique as ocorrências e a CONTRATANTE aceite tais justificativas.

6.2.2. Serviço de mitigação de ataques de negação de serviço (DDoS)

6.2.2.1. REQUISITOS MÍNIMOS

- a) A assinatura mensal de Anti-DDoS **compõe o Link dedicado de acesso a internet** descrito neste lote;
- b) A CONTRATADA deverá disponibilizar proteção contra ataques de negação de serviço, evitando assim a saturação da banda da Internet e indisponibilidade dos serviços em momentos de ataques DOS (denial of service) e DDoS (distributed denial of service);
- c) O acesso à internet não poderá ser subcontratado de terceiros, devendo a CONTRATADA fornecer ambos os serviços, solução anti-DDoS e circuito de dados;
- d) A técnica anti-DDoS utilizada deverá ser por métrica de volumetria, assim a contratada deverá enviar junto com a proposta técnica, qual a estratégia utilizada para mitigação de ataques DDoS sobre o circuito de dados;
- e) A solução anti-DDoS deverá prover o serviço de mitigação de ataques de negação de serviço DoS, sejam eles DDoS ou não;
- f) A CONTRATADA deve possuir e disponibilizar no mínimo 02 (dois) centros de limpeza nacional cada um com capacidade de mitigação de no mínimo 10Gbps e no mínimo 01 (um) centro de limpeza internacional com capacidade de mitigação de no mínimo 10 GBPS;
- g) Não haverá taxa adicional para a CONTRATADA por volume de mitigação de ataques DDoS nos IP monitorados;
- h) A alteração de capacidade de mitigação deverá ser implementada em um prazo máximo de 5 dias úteis, a contar da data de solicitação formal através de correio eletrônico encaminhado via chave oficial ou de autorizados pela CONTRATANTE;
- i) O ataque deve ser mitigado separando o tráfego legítimo do malicioso, de modo que os serviços de providos pelo cliente continuem disponíveis;
- j) A limpeza do tráfego deverá ser seletiva e atuar somente sobre os pacotes destinados ao IP atacado, todo tráfego restante não deverá sofrer nenhuma forma de limpeza ou desvio;
- k) A solução deve possuir mecanismos para filtragem de pacotes anômalos, garantindo a validade das conexões, sem efetuar qualquer limitação com base no número de sessões ou de pacotes por endereço, de modo a evitar o bloqueio de usuários legítimos;
- l) A CONTRATADA deve tomar todas as providências necessárias para recompor a disponibilidade do link em caso de incidentes de ataques de DDoS, recuperando o pleno funcionamento do mesmo;
- m) O envio de tráfego para mitigação em centros internacionais deverá ser justificado em relatório;
- n) Nos períodos de ataque a latência do circuito deverá ser de no máximo 100 ms (milissegundos) quando a mitigação se originar dos centros de limpeza nacionais e de no máximo 250 ms (milissegundos) quando se originar dos centros internacionais;
- o) A solução deverá possuir funcionalidades de monitoramento, detecção e mitigação de ataques, demandas em operação ininterrupta durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual;
- p) A análise realizada para fins da solução deverá ser passiva sem utilização de elementos da rede da contratante para coletas dos dados a serem analisados;
- q) A mitigação de ataques deve ser baseada em arquitetura na qual há o desvio de tráfego suspeito comandado pelo equipamento de monitoramento, por meio de alterações do plano de roteamento;

r) A solução deve manter uma lista dinâmica de endereços IP bloqueados, revisando dessa lista os endereços que não enviarem mais requisições maliciosas após um período de tempo considerado seguro por um determinado cliente;

s) A solução deve suportar a mitigação automática de ataques, utilizando múltiplas técnicas como White Lists, Black Lists, limitação de taxa, técnicas desafio-resposta, descarte de pacotes malformados, técnicas de mitigação de ataques aos protocolos HTTP/HTTPS, DNS, VPN, FTP, NTP, UDP, ICMP, correio eletrônico, bloqueio por localização geográfica de endereços IP, dentre outras;

t) A solução deve implementar mecanismos capazes de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede, para protocolo IPv4, incluindo, mas não se restringindo aos seguintes:

- Ataques de inundação (Bandwidth Flood), incluindo Flood de UDP e ICMP;

- Ataques à pilha TCP, incluindo mau-uso das Flags TCP, ataques de RST e FIN, SYN Flood e TCP

Idle Resets;

- Ataques que utilizam a fragmentação de pacotes, incluindo pacotes IP, TCP e UDP;

Spoofing);

- Ataques de botnets, worms e ataques que utilizam falsificação de endereços IP origem (IP

u) Em nenhum caso será aceito bloqueio de ataques de DOS e DDOS por ACLs em roteadores de bordas da contratada;

v) Caso o volume de tráfego do ataque ultrapasse as capacidades de mitigação especificadas ou sature as conexões do AS, devem ser tomadas contramedidas tais como aquelas que permitam o bloqueio seletivo por blocos de IP de origem no AS pelo qual o ataque esteja ocorrendo, utilizando técnicas como Remote Triggered Black Hole;

w) Realizar a comunicação da ocorrência do ataque à CONTRATANTE imediatamente após a detecção;

x) A CONTRATADA deverá disponibilizar relatórios mensais de mitigação de ataques, contendo no mínimo horário de início do ataque, horário de início de ação de mitigação, horário de sucesso da mitigação e horário de fim do ataque. Em conjunto com o relatório mensal relatórios dinâmicos deverão ser disponibilizados em até 48 horas após um ataque por solicitação da CONTRATANTE;

y) A CONTRATADA deverá comprovar por meio de Atestado de Capacidade Técnica, fornecido por pessoa jurídica de direito público ou privado, declarando ter a empresa licitante fornecido ou estarem fornecendo serviço de limpeza contra-ataques DDOS (Distributed Denial of Service);

z) A CONTRATADA deverá apresentar relatório analítico, enviado mensalmente ao cliente;

aa) A CONTRATADA deverá disponibilizar 02 (dois) Centro Operacional de Segurança no Brasil, com equipe especializada em monitoramento, detecção e mitigação de ataques, em idioma português brasileiro, durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual;

ab) A CONTRATADA terá no máximo 15 minutos para iniciar a mitigação de ataques de DOS e DDOS.

6.3. LOTE II

6.3.1. Serviço de Link dedicado de acesso a internet (Redundância)

6.3.1.1. REQUISITOS MÍNIMOS

a) O link deverá ser provido no datacenter da SEFAZ/AC, na velocidade de 5 Gbps.

b) A CONTRATADA deverá fornecer no mínimo 64 endereços IP válidos na internet;

c) Os endereços IP deverão ser reservados pela CONTRATADA exclusivamente para a CONTRATANTE, independente de utilização;

d) Deverá ser disponibilizado acesso permanente que possibilite a interligação do ambiente da CONTRATANTE à rede mundial de computadores, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, composto de um canal direto com a Internet de uso ilimitado, em conformidade com os prazos definidos no Acordo de Nível de Serviço;

- e) O acesso não poderá ser compartilhado com nenhum outro cliente da CONTRATADA e deverá ser capaz de absorver 100% (cem por cento) do tráfego referente à velocidade contratada;
- f) O backbone ofertado deverá possuir, a partir da cidade de Rio Branco/AC, no mínimo duas abordagens físicas e lógicas distintas própria ou de terceiros, desde comprovada que a largura de banda atenda o dobro da solicitação da SEFAZ, garantindo rotas redundantes para a saída de tráfego nacional e internacional, de modo a assegurar a alta disponibilidade e a continuidade do serviço.
- g) A CONTRATADA deverá possuir saída de backbone internacional com capacidade de transmissão de pelo menos 10 Gbps;
- h) Todo fornecimento e instalação dos materiais e equipamentos necessários à prestação dos serviços pela CONTRATADA, não poderá acarretar ônus adicional à CONTRATANTE, logo, deverão estar inclusos na solução todos os recursos de conectividade, tais como: modems, conversores, roteadores, e outros correlatos necessários à prestação dos serviços, exceto racks e tomadas de energia;
- i) Os equipamentos fornecidos deverão ser capazes de atender INTEGRALMENTE aos requisitos de qualidade e velocidade do link de comunicação de dados contratado;
- j) Os roteadores integrantes do backbone da prestadora de serviços e os roteadores instalados no datacenter da CONTRATANTE deverão possuir capacidade de suportar o tráfego com banda completamente ocupada, sem que os limites de 70% de utilização da CPU sejam excedidos;
- k) Os recursos de hardware e software dos equipamentos devem ser atualizados tecnologicamente, sem ônus para a CONTRATANTE, durante a vigência do contrato;
- l) Os equipamentos fornecidos deverão permitir a instalação em rack de 19 polegadas, devendo vir acompanhado de todas as peças e acessórios necessários para fixação;
- m) Os equipamentos fornecidos deverão possuir fonte de alimentação redundante com entrada 110/220 volts AC e com a frequência de 60 Hz, com comutação automática de tensão;
- n) Os equipamentos fornecidos deverão acompanhar todos os acessórios necessários para operacionalização do equipamento (softwares, sistemas operacionais, cabos lógicos de gerenciamento/console, cabos de energia elétrica seguindo o novo padrão brasileiro de tomadas);
- o) O equipamento de entrega de última milha deve possuir pelo menos 2 (duas) interfaces 10 Gigabit Ethernet com conector SFP+ e transceiver compatível com o equipamento instalado na SEFAZ/AC para entrada de links (FORTIGATE 401F) e 1 (uma) interface Gigabit Ethernet com conector RJ-45. Todos os cabos necessários para conexão entre os equipamentos serão de responsabilidade da CONTRATADA;
- p) Sempre que houver lançamento de nova versão estável de sistema operacional e ou firmware que faça correções de segurança dos equipamentos fornecidos, a CONTRATADA deverá providenciar as atualizações com prévia aprovação da CONTRATANTE, sem ônus adicional;
- q) O link e equipamentos fornecidos pela CONTRATADA, nas suas condições de fabricação, operação, manutenção, configuração, funcionamento, alimentação e instalação, deverão obedecer rigorosamente às normas e recomendações em vigor, elaboradas por órgãos oficiais competentes ou entidades autônomas reconhecidas na área – ABNT (Associação Brasileira de Normas Técnicas) e ANATEL (Agência Nacional de Telecomunicações), e entidades de padrões reconhecidas internacionalmente – ITU-T (Internacional Telecommunication Union), ISO (International Standardization Organization), IEEE (Institute of Electrical and Electronics Engineers), EIA/TIA (Electronics Industry Alliance and Telecommunication Industry Association);
- r) A CONTRATADA deverá fornecer as senhas de acesso, via porta de console e via SSHv2, para cada um dos roteadores instalados, com privilégios somente para operações de leitura – (read only) para os comandos “ping”, “tracert” e “trace”. Também deverá ser fornecido acesso somente de leitura às estatísticas de SNMP (comunidade de leitura ou usuário/senha), além de configurar os roteadores para gerar logs (Syslog – RFC 3164) e/ou traps SNMP para um ou mais endereços IPs a serem definidos pela CONTRATANTE;
- s) Todo conjunto de materiais e equipamentos fornecidos pela CONTRATADA, deverão ser novos e sem uso prévio, atendendo as normas do Código de Defesa do Consumidor, não podendo ser reciclados ou recondicionados e nem de fabricação artesanal;
- t) Deverá dispor de reserva técnica de componentes sobressalentes suficientes, caso haja necessidade de substituição;

u) Todo e qualquer equipamento, acessório ou interface, ainda que não mencionados neste documento, porém, necessário à composição da solução ou necessário ao atendimento de qualquer funcionalidade ou configuração requerida neste documento deverá estar incluída na solução proposta, sem implicação de ônus adicional para a CONTRATANTE;

v) Os equipamentos que se mostrarem necessários deverão ser fornecidos pela CONTRATADA, em regime de comodato;

6.3.1.2. ESCALABILIDADE

a) Ajuste Dinâmico de Largura de Banda: A infraestrutura de um link dedicado permite ajustes dinâmicos na largura de banda, permitindo escalabilidade conforme as necessidades de crescimento da empresa;

b) O circuito deverá permitir aumento de velocidade e troca de rotas, de acordo com a demanda futura da SEFAZ, o que poderá ser objeto de aditivo contratual, nos termos e limites legais;

c) O tempo máximo para alteração da velocidade de acesso deverá ser de 05 (cinco) dias úteis após a assinatura do correspondente termo aditivo ao contrato;

d) No caso de aumento da velocidade do link de comunicação (upgrade), será permitida a substituição do equipamento/roteador e/ou interface de conexão para que o serviço continue sendo prestado em conformidade com o previsto neste Termo.

6.3.1.3. PENALIDADES

a) As penalidades abaixo serão aplicadas sobre os valores individuais de cada acesso analisado e constarão na fatura mensal do período subsequente ao da (s) ocorrência (s). No caso de descumprimento, pela CONTRATADA, de mais de um Nível de Serviço acordado, num mesmo período, num determinado acesso, as penalidades serão somadas até o valor máximo de 100% (cem por cento):

- Taxa de erros média mensal (mínimo de dez amostras, em dias distintos) maior que a contratada: 10%

- Prazo de instalação ou de mudança de endereço de instalação ou de mudança de velocidade maior que o contratado: 10% + 0,5% por dia inteiro de atraso;

- Prazo para recuperação/reparação do serviço maior que o contratado: 10% + 1% por hora inteira de atraso;

- Nota: As penalidades poderão ser reduzidas ou anuladas caso a CONTRATADA justifique as ocorrências e a CONTRATANTE aceite tais justificativas.

6.3.2. Serviço de mitigação de ataques de negação de serviço (DDoS)

6.3.2.1. REQUISITOS MÍNIMOS

a) A assinatura mensal de Anti-DDoS **compõe o Link dedicado de acesso a internet** descrito neste lote;

b) A CONTRATADA deverá disponibilizar proteção contra ataques de negação de serviço, evitando assim a saturação da banda da Internet e indisponibilidade dos serviços em momentos de ataques DOS (denial of service) e DDOS (distributed denial of service);

c) O acesso à internet não poderá ser subcontratado de terceiros, devendo a CONTRATADA fornecer ambos os serviços, solução anti-DDoS e circuito de dados;

d) A técnica anti-DDoS utilizada deverá ser por métrica de volumetria, assim a contratada deverá enviar junto com a proposta técnica, qual a estratégia utilizada para mitigação de ataques DDOS sobre o circuito de dados;

e) A solução anti-DDoS deverá prover o serviço de mitigação de ataques de negação de serviço DoS, sejam eles DDOS ou não;

f) A CONTRATADA deve possuir e disponibilizar no mínimo 02 (dois) centros de limpeza nacional cada um com capacidade de mitigação de no mínimo 10Gbps e no mínimo 01 (um) centro de limpeza internacional com capacidade de mitigação de no mínimo 10 GBPS;

g) Não haverá taxa adicional para a CONTRATADA por volume de mitigação de ataques DDOS nos IP monitorados;

h) A alteração de capacidade de mitigação deverá ser implementada em um prazo máximo de 5 dias úteis, a contar da data de solicitação formal através de correio eletrônico encaminhado via chave oficial ou de autorizados pela CONTRATANTE;

i) O ataque deve ser mitigado separando o tráfego legítimo do malicioso, de modo que os serviços de providos pelo cliente continuem disponíveis;

j) A limpeza do tráfego deverá ser seletiva e atuar somente sobre os pacotes destinados ao IP atacado, todo tráfego restante não deverá sofrer nenhuma forma de limpeza ou desvio;

k) A solução deve possuir mecanismos para filtragem de pacotes anômalos, garantindo a validade das conexões, sem efetuar qualquer limitação com base no número de sessões ou de pacotes por endereço, de modo a evitar o bloqueio de usuários legítimos;

l) A CONTRATADA deve tomar todas as providências necessárias para recompor a disponibilidade do link em caso de incidentes de ataques de DDoS, recuperando o pleno funcionamento do mesmo;

m) O envio de tráfego para mitigação em centros internacionais deverá ser justificado em relatório;

n) Nos períodos de ataque a latência do circuito deverá ser de no máximo 100 ms (milissegundos) quando a mitigação se originar dos centros de limpeza nacionais e de no máximo 250 ms (milissegundos) quando se originar dos centros internacionais;

o) A solução deverá possuir funcionalidades de monitoramento, detecção e mitigação de ataques, demandas em operação ininterrupta durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual;

p) A análise realizada para fins da solução deverá ser passiva sem utilização de elementos da rede da contratante para coletas dos dados a serem analisados;

q) A mitigação de ataques deve ser baseada em arquitetura na qual há o desvio de tráfego suspeito comandado pelo equipamento de monitoramento, por meio de alterações do plano de roteamento;

r) A solução deve manter uma lista dinâmica de endereços IP bloqueados, revisando dessa lista os endereços que não enviarem mais requisições maliciosas após um período de tempo considerado seguro por um determinado cliente;

s) A solução deve suportar a mitigação automática de ataques, utilizando múltiplas técnicas como White Lists, Black Lists, limitação de taxa, técnicas desafio-resposta, descarte de pacotes malformados, técnicas de mitigação de ataques aos protocolos HTTP/HTTPS, DNS, VPN, FTP, NTP, UDP, ICMP, correio eletrônico, bloqueio por localização geográfica de endereços IP, dentre outras;

t) A solução deve implementar mecanismos capazes de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede, para protocolo IPv4, incluindo, mas não se restringindo aos seguintes:

- Ataques de inundação (Bandwidth Flood), incluindo Flood de UDP e ICMP;

- Ataques à pilha TCP, incluindo mau-uso das Flags TCP, ataques de RST e FIN, SYN Flood e TCP

Idle Resets;

- Ataques que utilizam a fragmentação de pacotes, incluindo pacotes IP, TCP e UDP;

- Ataques de botnets, worms e ataques que utilizam falsificação de endereços IP origem (IP

Spoofing);

u) Em nenhum caso será aceito bloqueio de ataques de DOS e DDOS por ACLs em roteadores de bordas da contratada;

v) Caso o volume de tráfego do ataque ultrapasse as capacidades de mitigação especificadas ou sature as conexões do AS, devem ser tomadas contramedidas tais como aquelas que permitam o bloqueio seletivo por blocos de IP de origem no AS pelo qual o ataque esteja ocorrendo, utilizando técnicas como Remote Triggered Black Hole;

w) Realizar a comunicação da ocorrência do ataque à CONTRATANTE imediatamente após a detecção;

x) A CONTRATADA deverá disponibilizar relatórios mensais de mitigação de ataques, contendo no mínimo horário de início do ataque, horário de início de ação de mitigação, horário de sucesso

da mitigação e horário de fim do ataque. Em conjunto com o relatório mensal relatórios dinâmicos deverão ser disponibilizados em até 48 horas após um ataque por solicitação da CONTRATANTE;

y) A CONTRATADA deverá comprovar por meio de Atestado de Capacidade Técnica, fornecido por pessoa jurídica de direito público ou privado, declarando ter a empresa licitante fornecido ou estarem fornecendo serviço de limpeza contra-ataques DDOS (Distributed Denial of Service);

z) A CONTRATADA deverá apresentar relatório analítico, enviado mensalmente ao cliente;

aa) A CONTRATADA deverá disponibilizar 02 (dois) Centro Operacional de Segurança no Brasil, com equipe especializada em monitoramento, detecção e mitigação de ataques, em idioma português brasileiro, durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual;

- A CONTRATADA terá no máximo 15 minutos para iniciar a mitigação de ataques de DOS e DDOS.

6.4. **LOTE III**

6.4.1. **Solução de segurança de perímetro - FG-401F/FORTINET**

6.4.1.1. **REQUISITOS MÍNIMOS DE HARDWARE E DESEMPENHO**

- a) Quantidade de interfaces para HA padrão 1 Gbps RJ45 ou SFP: mínimo 2 interfaces;
- b) Quantidade de interfaces padrão 1 GE RJ45: mínimo 16 interfaces;
- c) Quantidade de interfaces padrão que suportem 1 GE SFP/SFP+: mínimo de 8 interfaces;
- d) Quantidade de interfaces padrão que suportem 10 GE SFP+: mínimo de 8 interfaces;
- e) Sessões simultâneas: mínimo de 7.500.000 sessões;
- f) Novas Sessões por segundo: mínimo de 450.000 por segundo;
- g) Throughput de IPsec VPN: mínimo de 50 Gbps;
- h) Quantidade de Túneis IPsec VPN concorrentes: mínimo de 2.000;
- i) Throughput com todas as proteções (Controle de Aplicação, IPS, Antivírus/Malware de FireWall) ativadas: mínimo de 9 Gbps;
- j) Desempenho mínimo em modo de Inspeção (descriptorgrafia e afia) de tráfego criptografado SSL de 7 Gbps. Os desempenhos devem ser comprovados por documento de domínio público. Não serão aceitas declarações ou cartas de fabricantes como comprovação deste item;
- k) Não serão aceitos o uso de cabo/interface do tipo breakout para contabilizar as quantidades de interfaces ethernet;
- l) Armazenamento interno redundante: armazenamento mínimo de 2 unidades de 480 Gb SSD;
- m) O equipamento deve possuir no mínimo 1 (uma) porta padrão USB de e para configuração e gerenciamento por interface de linha de comando;
- n) Fonte de alimentação: 220V redundante, o equipamento deverá ser capaz de operar com uma única fonte de alimentação.

6.4.1.2. **LICENCIAMENTO E SUPORTE TÉCNICO**

- a) Todos os equipamentos, produtos, peças ou software ofertados deverão ser novos e de primeiro uso e não constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support ou end-of-life do fabricante, ou seja, não deverão ter previsão de descontinuidade de serviço, suporte ou vida, devendo estar em linha de produção do fabricante e cobertos por contratos de suporte e atualização de versão do fabricante pelo período mínimo de 60 (sessenta) meses;
- b) Os equipamentos que se mostrarem necessários deverão ser fornecidos pela CONTRATADA, em regime de comodato;
- c) A solução de firewall deve possuir suporte, durante todo o período contratual, compreendendo a reposição de peças/equipamentos, atualizações do sistema operacional do equipamento e demais software e das assinaturas de proteção da solução.
- d) Durante o período contratual, deve ser possível realizar a atualização de sistema operacional dos equipamentos para obter novas funcionalidades e correção de bugs;

- e) Em caso de defeitos de fabricação, a CONTRATADA deve incluir envio de peças ou equipamentos de reposição, obedecendo à modalidade NBD (Next Business Day);
- f) Os chamados deverão ser abertos diretamente com a CONTRATADA;
- g) A empresa contratada deverá disponibilizar, estrutura de suporte técnico por meio de atendimento telefônico ou website ou e-mail;
- h) A contratada deverá disponibilizar um portal web com disponibilidade de 24 horas por dia, 7 dias por semana, com sistema de help-desk para abertura de chamados de suporte técnico;
- i) A equipe técnica da CONTRATANTE poderá abrir, gerenciar status e conferir todo o histórico de chamados de suporte técnico, mediante login e senha de acesso ao sistema;
- j) Todo o chamado aberto deverá ter sua resolução técnica registrada no sistema web de help-desk;
- k) A contratada deve indicar, por ocasião do início dos trabalhos, os procedimentos para abertura de suporte técnico;
- l) Todas as funcionalidades adquiridas de hardware e software devem operar conforme disposto neste Termo de Referência durante o período contratual, ou seja, o fornecedor deve garantir a atualização completa das funcionalidades, não sendo permitida a cobrança de quaisquer valores adicionais pelo uso dos hardwares e softwares para esse período.

6.4.1.3. FUNCIONALIDADES MÍNIMAS DO EQUIPAMENTO

- a) Todas as funcionalidades e requisitos de desempenho descritas neste termo de referência devem estar devidamente licenciadas para o período total do contrato;
- b) As funcionalidades de IPS, Antivírus e Controle de Aplicação devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado;
- c) A CONTRATADA deverá implementar a funcionalidade de alta disponibilidade (HA) em modo ativo/passivo, de modo que apenas um dos appliance suporte todas as funcionalidades e requisitos de desempenho exigidos neste termo de referência.
- d) Não será permitido a utilização de clusters ou tecnologias equivalentes os quais somados alcancem o total de portas e desempenho solicitado.
- e) A CONTRATANTE terá a liberdade de escolher durante o contrato administrativo se deseja implementar os NGFWs em modo Ativo/Ativo ou Ativo/Passivo, não sendo permitido o fornecimento de licenças que obrigue o funcionamento dos NGFWs somente em modo Ativo/Passivo;
- f) A solução deve consistir de appliance de proteção de rede com funcionalidades, licenciadas por todo período contratual, de Next Generation Firewall (NGFW) tais como:
 - Reconhecimento e identificação e controle de aplicações;
 - Identificação de usuários através de LDAP e RADIUS;
 - Prevenção contra ameaças de vírus spywares e malwares desconhecidos (Zero Day);
 - IPS (Intrusion Prevention System);
 - Filtro de URL (Web);
 - VPN;
 - Inspeção de SSL e SSH;
 - Filtro de DNS;
 - Deve possuir funcionalidade de políticas baseada em rotas, permitindo que se defina uma rota estática a uma interface de rede;
 - Possuir sistema de segurança com aplicação de filtros de pacotes baseados em regras, estados de conexão e inspeção profunda de pacotes, licenciadas por todo período contratual.
- g) Deve customizar para a CONTRATANTE todas as páginas web que porventura interajam com o usuário;
- h) As imagens e textos necessários serão fornecidos pela equipe técnica da CONTRATANTE;

- i) Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes ou baseado em usuários ou grupo de usuários (traffic shaping);
- j) Emitir alertas via correio eletrônico, syslog e traps SNMP;
- k) Deve possuir MIB própria contemplando, no mínimo, indicadores de estado do hardware e interfaces WAN e performance do equipamento;
- l) Possuir, no mínimo, suporte a SNMP v2 e v3;
- m) Deve suportar, no próprio firewall, autenticação de usuários locais e integração com serviços de autenticação de diretório LDAP, Microsoft Active Directory e RADIUS;
- n) Suportar e efetuar a captura de pacotes e exportação no formato PCAP;
- o) Suportar tags de VLAN, IEEE 802.1Q;
- p) O equipamento deve ser fornecido em hardware dedicado, novo e de primeiro uso, tipo appliance com sistema operacional otimizado, do mesmo fabricante, para o uso como firewall corporativo multifuncional;
- q) Prover servidor DHCP interno suportando no mínimo um escopo por interface e a funcionalidade de DHCP Relay;
- r) Prover mecanismo de conversão de endereços NAT (Network Address Translation) e PAT (Port Address Translation);
- s) Possuir suporte a redes IPv6 e IPv4;
- t) Possuir o gerenciamento de tráfego de entrada e saída por serviços, endereços IP e regra de firewall, permitindo definir banda mínima garantida e máxima permitida;
- u) Implementar os serviços de Provedor VPN baseado no protocolo IPsec, com certificação digital;
- v) Não serão permitidas soluções baseadas em redirecionamento de tráfego para dispositivos externos ao appliance para análise de arquivos ou pacotes;
- w) O equipamento fornecido deve ser próprio para montagem em rack 19", com altura máxima de 3Us, incluindo kit para adaptação, se necessário, e cabos de alimentação;
- x) Deve possuir o recurso de agregação de links conforme padrão IEEE 802.3ad (LACP) permitindo o agrupamento de interfaces físicas de rede em um link agrupado virtualmente (LAG – Link Aggregation Group);
- y) Suportar, no mínimo, os protocolos de roteamento dinâmico OSPF v3 e BGP, bem como as funcionalidades de roteamento estático e roteamento policy-based;
- z) Deve permitir o envio de logs para sistemas de monitoração externos utilizando o padrão syslog, bem como o envio de forma segura através do protocolo SSL/TLS ou outro protocolo que implementa segurança na transferência dos arquivos;
- aa) Deve implementar controle por políticas/regras de firewall capaz de permitir ou bloquear o tráfego de rede por:
 - Porta e protocolo;
 - Aplicações, grupos estáticos de aplicações, por grupos dinâmicos de aplicações baseados em características e comportamento das aplicações;
 - Usuários e grupos de usuários;
 - Endereços IP e faixas de endereços IP e por país de origem e destino do tráfego.
- ab) Deve possuir a capacidade para realizar a decriptografia do tráfego SSL e SSH permitindo o controle e inspeção tanto do tráfego de entrada quanto de saída. A decriptografia deve ser realizada com base em políticas/regras de acordo com a origem e destino do tráfego;
- ac) Deve possuir recurso de QoS – Quality of Service com suporte a DSCP – Differentiated Services Code Point. Deve permitir também definir, baseado em políticas/regras, a prioridade e o limite máximo de largura de banda de um determinado tipo de tráfego. As definições de prioridade e limite de largura de banda devem ser baseadas no endereço IP de origem e destino, no usuário e na aplicação;

ad)A solução de firewall deve possuir integração com LDAP, MS Active Directory e RADIUS para identificação dos usuários e grupos da rede para uso nas políticas/regras baseadas por usuários e grupo de usuários;

ae)Deve ter a integração com LDAP, MS Active Directory, RADIUS e a Item VIII - Solução De Autenticação De Usuários e Dispositivos (NAC), constante neste termo de referência para identificação dos usuários e grupos da rede para implementação de Single sign-on (SSO);

af)Deve ser possível criar perfis de acesso à interface de gerenciamento com permissões granulares como acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações entre outros;

ag)Deve permitir realizar o backup das configurações do equipamento e a restauração da configuração salva através de interface de gerenciamento;

ah)Por cada equipamento que compõe a solução de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;

ai) Deve possuir a capacidade de reconhecer aplicações diferentes tais como redes sociais, compartilhamento de arquivos, e-mail, atualização de softwares, acesso remoto, VoIP, áudio e vídeo, peer-to-peer, sistemas de mensagem instantânea etc., sendo está uma lista não exaustiva;

aj) O reconhecimento da aplicação se dará, independentemente de porta e protocolo, através de, no mínimo, os seguintes métodos:

- Baseado na assinatura da aplicação conhecida pelo fabricante da solução de firewall ou através da decodificação de protocolos para detectar aplicações encapsuladas dentro do protocolo ou identificação através de análise heurística a fim de

- detectar aplicações através de análise comportamental do tráfego analisado;

- Deve permitir a diferenciação e controle de partes da aplicação como, por exemplo, em uma aplicação de mensagem instantânea permitir a troca de mensagens de texto e bloquear a transferência de arquivos por dentro da aplicação;

- Deve permitir bloquear sessões TCP que utilizarem variações do three-way handshake, prevenindo assim possíveis tráfegos maliciosos;

- Deve permitir bloquear conexões que contenham dados no payload dos pacotes TCP SYN e TCP SYN-ACK durante o three-way handshake.

ak)A solução de firewall deve possuir funcionalidades de IPS, antivírus e anti-spyware que permita o bloqueio de vulnerabilidades e exploits conhecidos e proteção contra vírus e spywares baseado em assinaturas de ameaças conhecidas;

al) Deve ser possível a criação de assinaturas customizadas de ameaças;

am)Deve permitir realizar o bloqueio de vírus realizando a inspeção em, no mínimo, os protocolos HTTP, FTP, SMB, SMTP e POP3. Será permitido o uso de appliance externo para o bloqueio de vírus caso a solução de firewall ofertada não realize nativamente a inspeção em algum dos protocolos solicitados;

an)Deve possuir a capacidade de detectar e prevenir ameaças em tráfego HTTP/2;

ao)Deve possuir proteção contra ataques de negação de serviço (DoS) capaz de impedir ataques de SYN Flood, ICMP Flood, UDP Flood, etc e deve também bloquear port scans, bloquear ataques de buffer overflow e identificar e bloquear comunicação com botnets;

ap)Para cada ameaça detectada pela solução deve ser realizado o registro nos logs do sistema das informações de data e hora, tipo da ameaça, origem e destino da comunicação e a ação tomada (se permitiu ou bloqueou o tráfego);

aq)A solução de firewall deve possuir funcionalidade de filtro URL que permita a criação de políticas/regras para controle do acesso a websites baseado em categorias de URL devendo o fabricante da solução disponibilizar a base de dados de URL categorizadas para consulta por parte da solução. As políticas/regras que permitem ou bloqueiam o acesso a determinada categoria de URL devem ser com base no usuário e grupos de usuários e por endereços IP e faixas de endereços IP;

ar) Deve permitir a criação de categoria de URL customizada permitindo inserir uma lista de URLs específicas;

as) Deve permitir a customização da página de bloqueio exibida ao usuário quando o mesmo tentar realizar um acesso a um website pertencente a uma categoria de URLs bloqueada;

at) A solução de firewall deve possuir recurso de portal de autenticação prévia (Captive Portal) para identificação dos usuários que realizam o acesso à internet, sem a necessidade de instalação de software cliente ou agente no computador. O portal de autenticação deve ser exibido antes de o usuário iniciar a navegação pela internet;

au) A solução de firewall deve possuir o recurso de VPN – Virtual Private Network dos tipos site-to-site e client-to-site e suportar IPSEC – Internet Protocol Security;

av) A solução de firewall deve possuir o recurso de VPN IPsec site-to-site dial-up;

aw) Deve suportar a autenticação dos usuários remotos que se conectam à VPN via LDAP, MS Active Directory, RADIUS e através de base de usuários local no equipamento da solução de firewall. Deve suportar também a autenticação via certificado;

ax) Deve ser disponibilizado o software cliente de VPN do mesmo fabricante da solução de firewall ofertada compatível para instalação em computadores com sistema operacional, MS Windows 10, MacOS e Linux e para instalação em dispositivos móveis Android e IOS;

ay) A solução de firewall deve possuir console de gerenciamento do equipamento acessada através de interface gráfica web, ou aplicação cliente-servidor do próprio fabricante para acesso à console de gerenciamento, permitindo realizar as configurações da solução como criar e administrar as políticas/regras de firewall e controle de aplicações, criar e administrar as políticas de IPS, antivírus e anti-spyware, criar e administrar as políticas de filtro URL, monitorar e investigar os registros de logs de eventos e demais configurações.

az) O console de gerenciamento do equipamento deve estar instalado no próprio appliance, não sendo permitido o uso de máquina física ou virtual externa para acesso ao gerenciamento do appliance;

ba) Permitir o bloqueio de programas exploradores de vulnerabilidades s) conhecidos;

bb) Incluir proteção contra ataques de negação de serviços (DoS);

bc) Possuir assinaturas específicas para a mitigação de ataques negação (DoS e DDoS);

bd) Deve ser possível através de interface ou console de gerenciamento do equipamento visualizar um resumo gráfico das aplicações utilizadas e ameaças vistas, principais aplicações por utilização de largura de banda, atividades de um usuário ou grupo de usuários específicos incluindo aplicações e URLs acessadas e permitir a criação de relatórios personalizados ou o envio de informações para solução de relatórios personalizados;

be) Deve ser exibida na interface gráfica de gerenciamento do equipamento informações em tempo real, atualizadas de forma automática, as principais aplicações acessadas, o risco das principais aplicações, número de sessões simultâneas, status das interfaces de rede e uso de CPU;

bf) Deve permitir configurar o agendamento das políticas/regras de firewall para habilitar ou desabilitar tais políticas/regras em horários pré-definidos;

bg) Devem estar licenciadas, para todo período contratual, as funcionalidades de prevenção contra ameaças de vírus, spywares e malwares desconhecidos (Zero Day), IPS, filtro de URL, controle de aplicações;

bh) Devem estar licenciadas, para todo período contratual, as quantidades mínimas de Túneis IPsec VPN concorrentes exigidos neste termo de referência;

bi) Caso sejam necessários licenciamentos para execução de arquivos no ambiente controlado (sandbox), os mesmos devem ser fornecidos em sua totalidade, sem custos adicionais para a CONTRATANTE;

bj) A solução para análise de malwares modernos (Sandbox) deve:

- Possuir funcionalidades, embarcadas no próprio appliance ou entregue em composição com outra solução virtual de mesmo fabricante, para análise de Malwares não conhecidos;

- Ser capaz de enviar arquivos trafegados de forma automática para análise em nuvem ou local, onde o arquivo será executado e simulado em ambiente controlado;

- Possibilitar a seleção, através de políticas granulares, de quais tipos de arquivos sofrerão a análise, incluindo, mas não limitado a:

endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;

bk) Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, no sistema operacional Windows 10 ou superior;

bl) Suportar a monitoração de arquivos trafegados na internet (HTTPs, FTP, HTTP, SMTP);

bm) Possuir sistema de análise capaz de prover informações sobre as ações do Malware na máquina infectada, gerar informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Anti spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover informações sobre o usuário infectado (Endereço IP e login de rede);

bn) Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;

bo) A solução deverá suportar e ser entregue licenciada para no mínimo 10 (dez) sistemas virtuais (contextos) de firewall.

6.4.1.4. RECURSOS GERAIS DE SD-WAN

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

b) Deve ser possível criar políticas que definam os critérios para match de Endereços de origem e Grupos de usuários;

c) Endereços de destino;

d) DSCP;

e) Aplicação de camada 7 utilizada (O365 Exchange, AWS, Dropbox e etc);

f) A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de health check, permitindo testes de resposta por ping, http, tcp/udp echo, dns, tcp-connect e twamp;

g) O SD-WAN deverá balancear o tráfego das aplicações entre múltiplos links simultaneamente;

h) A solução deve permitir a configuração e uso de várias interfaces SD-WAN. Cada uma com seus links;

i) O SD-WAN deverá analisar o tráfego em tempo real e realizar o balanceamento dos pacotes de um mesmo fluxo (sessão) entre múltiplos links simultaneamente;

j) Deve possuir suporte ao MOS (Mean Opinion Score), para calcular a qualidade de chamadas de voz, considerando jitter, perda de pacote e codec utilizado;

k) Deverá ser permitida a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote, banda ocupada ou todos ao mesmo tempo;

l) A solução de SD-WAN deve possibilitar o uso de túneis VPN dinâmicos, entre pontas remotas, para aplicações sensíveis. Uma vez que as pontas se trocam informações entre si, é feito by-pass do hub;

m) Deve permitir a segmentação de várias VRFs sobre um único túnel SD-WAN;

n) Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;

o) A solução deve permitir a definição do roteamento para cada aplicação;

p) Diversas formas de escolha do link devem estar presentes, incluindo: melhor link, menor custo e definição de níveis máximos de qualidade a serem aceitos para que tais links possam ser utilizados em um determinado roteamento de aplicação;

q) Deve possibilitar a definição do link de saída para uma aplicação específica;

r) Deve implementar balanceamento de link por hash do IP de origem;

s) Deve implementar balanceamento de link por hash do IP de origem e destino;

t) Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;

- u) Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;
- v) A solução de SD-WAN deve possuir suporte a Policy based routing ou policy based forwarding;
- w) Para IPv4, deve suportar roteamento estático e dinâmico (BGP e OSPF);
- x) Deve possuir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões. A solução deve realizar os ajustes dinâmicos na relação perda de pacote x envio de pacotes redundantes;
- y) Deve ser possível habilitar o FEC para tráfegos específicos. Ex: apenas para aplicações sensíveis a perda de pacote;
- z) Deve permitir a customização dos timers para detecção de queda de link, bem como tempo necessário para retornar com o link para o balanceamento após restabelecido;
- aa) A solução de SD-WAN deve suportar nativamente conectores com clouds públicas. Pelo menos: Azure, AWS e GCP;
- ab) Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, Facebook, etc), impactando no bom uso das aplicações de negócio, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de shaping;
- ac) Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem, endereço de destino, usuário e grupo de usuários, aplicações e porta;
- ad) O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;
- ae) O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como Youtube, Facebook etc;
- af) Deve ainda possibilitar a marcação de DSCP, a fim de que essa informação possa ser utilizada ao longo do backbone para fins de reserva de banda;
- ag) O QoS deve possibilitar a definição de fila de prioridade;
- ah) Além de possibilitar a definição de banda máxima e garantida por aplicação, deve também suportar o match em categorias de URL, IPs de origem e destino, logins e portas;
- ai) A capacidade de agendar intervalos de tempo em que as políticas de shaping/QoS serão válidas é mandatória. Ex: regra de controle de banda mais permissivas durante o horário de almoço;
- aj) Deve possibilitar a definição de bandas distintas para download e upload;
- ak) A solução de SD-WAN deve prover estatísticas em tempo real a respeito da ocupação de banda (upload e download) e performance do health check (packet loss, jitter e latência);
- al) A solução de SD-WAN deve suportar health check ativo, passivo e misto:
 - Ativo: criação manual de health check, definindo o destino a ser medido e o protocolo;
 - Passivo: uso do tráfego real para as medições;
 - Misto: Passivo quando há tráfego do usuário e, na ausência dele, chaveamento para o método ativo.
- am) A solução de SD-WAN deve suportar IPv6;
- an) Deve possibilitar roteamento distinto a depender do grupo de usuário selecionado na regra de SD-WAN;
- ao) Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;
- ap) O SD-WAN deverá possuir serviço de Firewall Stateful;
- aq) A solução SD-WAN deverá fornecer criptografia AES de 128 bits ou AES de 256 bits em sua VPN;
- ar) A solução SD-WAN deverá simplificar a implantação de túneis criptografados de site para site;
- as) Deve ser capaz de bloquear acesso às aplicações;
- at) Deve suportar NAT dinâmico bem como NAT de saída;

- au) Deve suportar balanceamento de tráfego por sessão e pacote;
- av) Suportar VPN IPSec Site-to-Site;
- aw) A VPN IPSEC deve suportar criptografia 3DES, AES128, AES192 e AES256 (Advanced Encryption Standard);
- ax) A VPN IPSEC deve suportar Autenticação MD5, SHA1, SHA256, SHA384 e SHA512;
- ay) A VPN IPSEC deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Group 15 até 21 e Group 27 até 32;
- az) A VPN IPSEC deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
- ba) A VPN IPSEC deve suportar Autenticação via certificado IKE PKI;
- bb) Deve suportar o uso de DDNS, para casos em que uma ou ambas as pontas possuam IPs dinâmicos;
- bc) O recurso de DDNS deve suportar IPv4 e IPv6;
- bd) Deve suportar VPN dial up, no caso da ponta remota não possui IP estático na WAN;
- be) Deve possuir suporte e estar licenciamento para uso de VRFs, em IPv4 e IPv6;
- bf) A solução de SD-WAN pode ser fornecida em composição com o firewall, desde que atenda aos mesmos requisitos de performance.

6.4.1.5. SOLUÇÃO SASE

- a) A solução deve permitir a conexão de no mínimo 250 usuários nesta plataforma;
- b) A gerência deve ser disponibilizada em nuvem, sem usar qualquer recurso do cliente;
- c) A solução SASE deve ser baseada em uma arquitetura em nuvem, permitindo a integração de funções de rede e segurança como serviço em uma única plataforma;
- d) O acesso a console de administração da solução SASE deve ser feito via navegador web e ter a possibilidade de se integrar com IdP para autenticação SSO dos usuários administrativos;
- e) A solução SASE deve garantir o acesso seguro à web, serviços em nuvem e aplicações privadas, independentemente da localização do usuário ou de onde essas aplicações estão hospedadas;
- f) A solução SASE deve ser (SaaS) software baseado em serviço que permite aos clientes acessarem a Internet com segurança e proteção. Deve garantir a proteção de endpoints e usuários remotos off-net (fora da rede) com o mesmo nível de segurança de quando estão na rede, independentemente de sua localização;
- g) A solução SASE deve ser composta por, no mínimo:
 - FWaaS (Firewall as a Service);
 - SWG (Secure Web Gateway);
 - CASB (Cloud Access Security Broker);
 - ZTNA (Zero Trust Network Access);
 - SD-WAN (Software-Defined Wide-Area Network);
 - DLP (Data Loss Prevention).
- h) Todos os componentes da solução SASE devem ser de um único fabricante, ou seja, deve ser uma solução Single-Vendor SASE (conforme definição cunhada pelo Gartner);
- i) A solução SASE deve ter cobertura mundial, com possibilidade de provisionamento nos seguintes continentes: Américas, Europa, África, Ásia e Oceania;
- j) A solução SASE deve permitir e estar licenciado para provisionamento em, no mínimo, 4 (quatro) pontos de presença (POP).
- k) Ao menos um ponto de presença deve estar disponível obrigatoriamente no Brasil;
- l) Os 4 (quatro) pontos de presença incluídos na solução SASE devem permitir a configuração de, no mínimo, 1 (um) endereço de IP fixo para cada. Caso a solução exija licenciamento adicional, este deve ser entregue para todos os POPs;

- m) A solução SASE deve possuir, além da redundância geográfica, a possibilidade de o usuário escolher em qual POP os logs serão armazenados para estar em compliance com legislações locais;
- n) A plataforma em nuvem da solução SASE deve ser monitorada e gerenciada 24 (vinte e quatro) horas por dia, 07 (sete) dias por semanas, com disponibilidade mensal de 99.999% para todos os serviços.
- o) A solução SASE deve possuir certificações SOC2, ISO 27001, ISO 27017 e ISO 27018;
- p) Quando um tráfego for direcionado a um POP da solução SASE, todo o processamento das funcionalidades de segurança deve acontecer dentro desse mesmo POP, sem que o tráfego seja direcionado para processamento, em cadeia, em diferentes datacenters.
- q) A comunicação entre agentes (clientes) e outras soluções de infraestrutura SASE devem sempre usar comunicação segura criptografada.
- r) A solução SASE deve permitir a integração com ambiente corporativo, escritórios, sites remotos através de SD-WAN Seguro.
- s) A solução SASE deve suportar os acessos:
- Acesso seguro à Internet (SIA) - com ou sem Agente;
 - Acesso Privado Seguro (SPA) – integração com outras arquiteturas que permitam o acesso privado seguro através de soluções como ZTNA, SD-WAN e NGFW para garantir eficiência e conectividade aos recursos locais;
 - As integrações com soluções NGFW devem ser feitas por comunicação criptografada e preferencialmente por túneis IPSec;
 - Acesso seguro a aplicações SaaS - Através da integração de API com provedores de nuvem, CASB deve adicionar controle e visibilidade aos dados e aplicações sancionados.
- t) A solução SASE deve permitir o acesso remoto seguro às aplicações hospedadas localmente (on-Premisse) através da integração de uma arquitetura SASE e ZTNA;
- u) A solução SASE deve permitir acesso seguro para aplicações em nuvem com CASB, adicionando mais controle, visibilidade das aplicações permitidas e dados de tráfego através de uma integração com a API do provedor;
- v) A solução SASE em conjunto com a arquitetura ZTNA deve permitir controle e análise profunda de postura do endpoint, permitindo o acesso apenas a partir de dispositivos seguros e as características específicas de cada acesso;
- w) A solução SASE, deve ter componente de Web Gateway Seguro com base de informações, inteligência, pesquisa e desenvolvimento de proteções com suporte a:
- Inspeção SSL;
 - Antivírus;
 - IPS;
 - Filtro Web baseado em categorias;
 - Proteção contra domínios de C&C;
 - Inline CASB;
 - Filtro de canais de Youtube.
- x) A solução SASE deve permitir o redirecionamento do tráfego web para uma solução de isolamento remoto de navegador (RBI), a partir de políticas de segurança que leve em consideração parâmetros tais como a categoria do site visitado e o usuário ou o seu grupo;
- y) Caso a solução SASE não possua nativamente uma solução de isolamento remoto de navegador (RBI), o licenciamento de uma solução do mesmo fabricante será permitido, desde que inclua o quantitativo de licenças para atender todos os clientes da solução SASE;
- z) O componente de isolamento remoto de navegador (RBI) deve possuir controle granular para bloquear ou permitir: clicar com o botão direito; imprimir para PDF; fazer o upload e/ou download de arquivos executáveis, de imagem, de texto e do Microsoft Office; copiar e colar textos;
- aa) Para acessos no formato SWG, sem cliente, a solução SASE deve possuir suporte para autenticação de usuários em diretório centralizado através de LDAP, Radius ou SAML;

ab)A solução SASE deve reconhecer o tráfego de rede gerado por um grande número de aplicações. O controle de aplicação com Inline-CASB deve usar decodificadores de protocolo que podem analisar o tráfego de rede para detectar o tráfego de aplicação, mesmo que o tráfego use portas ou protocolos não padrão. O Controle de Aplicação com Inline-CASB deve suportar a detecção de tráfego usando o protocolo HTTP (versões 1.0, 1.1 e 2.0);

ac)A solução SASE deve permitir a configuração e adição do Inline-CASB sob demanda, suportar o controle de aplicações SaaS através de inclusão de headers http e restrição de tenant tanto no uso com cliente quanto no uso sem cliente;

ad)A solução SASE deve suportar e estar licenciada para controlar, no mínimo, as seguintes aplicações SaaS:

- Microsoft Office 365;
- Microsoft OneDrive;
- Microsoft Teams;
- Outlook ou Hotmail;
- ChatGPT;
- Gmail;
- Google Workspace (Calendar, Docs, Drive, Meet);
- Meta (Facebook, Instagram);
- YouTube;
- DocuSign;
- GitHub;
- LinkedIn;
- Zoom.

ae)A solução SASE deve permitir a geração de relatórios e visualização de logs. Os relatórios e logs deverão informar sobre atividades de rede, detecção de vírus, visita a sites inválidos, intrusões, tentativas de falha de login, etc;

af) A solução SASE deve permitir gerar relatórios de dados a partir de logs. Deve permitir executar regularmente relatórios em intervalos programados e executar relatórios manualmente quando desejado;

ag)A solução SASE deve possuir módulo de logs para informações estatísticas e de segurança;

ah)A solução SASE deve permitir o encaminhamento de forma segura de logs para um servidor externo no formato Syslog ou CEF;

ai) Para acessos através de cliente, a solução SASE deve possuir suporte para autenticação de usuários em diretório centralizado através de LDAP, RADIUS ou SAML;

aj) A solução SASE deve gerar certificados que serão utilizados pelos Agentes para registro. Apenas certificados gerados pela solução deverão ser aceitos para validação;

ak)A solução SASE deve utilizar apenas 01 (um) Agente (Cliente) para a comunicação com a plataforma SASE, ZTNA e outros benefícios como Sandbox, AntiMalware, Varredura de Vulnerabilidades, Inventário de Software, Filtro Web, entre outros;

al) A solução SASE deve permitir que sejam aplicadas políticas de segurança de forma granular para o acesso seguro à Internet e para o acesso a aplicações internas em conjunto com o ZTNA ou Acesso Privado Seguro (SPA), com controle baseado em IP, Aplicação, Usuário ou Grupo de Usuários;

am)O Agente da solução SASE deve ser compatível com os seguintes Sistemas Operacionais: Windows, macOS, Linux, Android e iOS;

an)A solução SASE deve ter integração através do SAML com IdP's como Azure AD e Okta, facilitando a autenticação dos usuários para se conectarem ao ambiente SASE;

ao)O Agente da solução SASE deve ser implementado manualmente através do download e inclusão do "Código de Convite" para ativar as funcionalidades;

ap) Após o registro do Agente na solução SASE, deve ser possível usar diferentes usuários (um de cada vez) para estabelecer o túnel e enviar tráfego para o SASE;

aq) A solução SASE deve possuir o suporte à configuração de uma conexão sempre ativa. A configuração sempre ativa é opcional e customizada pelo administrador da solução;

ar) A solução SASE deve suportar a configuração do Acesso à Rede de Confiança Zero (ZTNA) sem instalação de Agente adicional (agentless ZTNA);

as) O acesso a aplicações via ZTNA sem agente deve suportar a configuração de aplicações privadas, que serão roteadas através do recurso Acesso Privado Seguro (SPA);

at) A solução SASE deve ter disponibilidade de pelo menos 1.0 Mbps de tráfego por usuário;

au) A solução SASE deve permitir o controle de mídias removíveis USB nos dispositivos finais;

av) A solução SASE deve permitir o acesso de aplicações privadas através de Proxy ZTNA em um NGFW;

aw) O cliente deve possuir funcionalidades de antivírus e envio de arquivos para análise de sandbox para proteção da estação caso o acesso à internet deixe de ser realizado de forma segura via SASE;

ax) A solução SASE deve permitir criação de regras de conformidade que avaliem a postura do dispositivo e auxiliem o administrador no controle de acesso, impedindo que um cliente não conforme possa se conectar a recursos;

ay) A postura deve ser monitorada continuamente para que, caso ocorra alguma alteração de conformidade, o acesso aos recursos possa ser bloqueado;

az) A solução SASE deve permitir a desativação ou ativação da análise de postura dos endpoints;

ba) Quando necessária a autenticação WEB para a solução SASE, as informações de login devem ser transmitidas por SSL e mantidas de forma segura;

bb) A solução de SASE deve ter console com módulos:

- Painéis de monitoramento;
- Configurações de Rede;
- Configurações SASE;
- Configurações do Sistema;
- Analytics que pode ser usado para análise em tempo real e elaboração de relatórios.
- A solução de SASE deve permitir criar e modificar o Dashboard (painel web) com matriz personalizável de widgets;
- A solução SASE deve incluir Dashboards (painéis) para monitorar o inventário de dispositivos, ameaças de segurança, tráfego e saúde da rede. Deve incluir os seguintes painéis:
 - Status: Fornece uma visão geral do seu ambiente SASE atual e do status do endpoint;
 - Mapa de Ativos: Exibe a localização geográfica dos ativos, incluindo servidores, em um mapa global. Também indica qual servidor tem o registro ativado;
 - Visão Única: Sistema abrangente de monitoramento para sua rede que integra dados em tempo real e históricos em uma única visualização.
 - Deve permitir usá-lo para registrar e monitorar ameaças às redes, filtrar dados em vários níveis e acompanhar a atividade administrativa.

bc) A solução SASE deve disponibilizar os seguintes monitores:

- Fontes: Exibe fontes por volume de tráfego e detalhamento por fonte;
- Thin-Edge: Exibe dispositivos Thin-Edge por volume de tráfego e detalhamento por dispositivo;
- Destinos: Exibe destinos por volume de tráfego e detalhamento por destino;
- Aplicações: Exibe aplicações por volume de tráfego e detalhamento por aplicação;
- Aplicações em Nuvem: Exibe aplicações em nuvem e detalhamento por aplicação;
- Sites da Web: Exibe sites por contagem de sessão e detalhamento por domínio;
- Políticas: Exibe políticas por volume de tráfego e detalhamento por número de política;

- Sessões: Exibe sessões por fonte de tráfego;
- VPN: Exibe conexões VPN por usuário;
- Ameaças: Exibe ameaças e detalhamento por ameaça.

bd)A solução SASE deve permitir visualizar os endpoints gerenciados através do widget de status correspondente ou do monitor de status. Tanto o widget quanto o monitor devem exibir gráficos que mostram informações do endpoint, incluindo o status e a plataforma. Deve permitir o cancelamento do registro de um endpoint a partir do widget ou monitor;

be)Para auxiliar os administradores no diagnóstico de problemas de conectividade e de performance de rede dos usuários remotos, a solução SASE deve incluir recursos de monitoramento fim-a-fim, desde o cliente da solução, passando pelo POP e até as aplicações de destino;

bf)A solução SASE deve permitir que monitoramentos sejam executados em tempo real e exibam as informações de consumo de CPU, memória e disco da estação cliente, além dos dados de performance de acesso (perda de pacotes e tempo de ida-volta (RTT)) à aplicação SaaS escolhida;

bg)A solução SASE deve permitir perfis administrativos específicos para administradores de leitura ou escrita;

bh)A solução SASE deve ter gerenciamento de implantação pela console da solução. Assim, implantações e atualizações de quaisquer soluções complementares podem ser obtidas através da nuvem;

bi)A solução SASE deve possuir suporte a segurança e filtros de DNS para os acessos via agente de forma a impedir ataques e acessos inseguros na camada de DNS;

bj)A solução SASE deve ter componente FWaaS (Firewall como Serviço) para aplicar políticas com Perfis que incluem Filtro Web, Antimalware, DLP, Filtro DNS, Filtro de Arquivos, IPS, Controle de APP e Inspeção SSL;

bk)A solução SASE deve ter mecanismo de prevenção de vazamento de dados para impedir que dados sensíveis saiam e entrem nos dispositivos protegidos;

bl)A solução SASE deve trazer dicionários de informações sensíveis, pré-definidos e atualizados automaticamente pelo fabricante, contendo no mínimo: números de cartões de crédito, códigos fonte Python, Java, Powershell e C, arquivos de configuração de equipamentos Cisco, CPF (Cadastro de Pessoa Física), CNPJ (Cadastro Nacional de Pessoa Jurídica) e CNH (Carteira Nacional de Habilitação);

bm)A solução SASE deve permitir a criação de dicionários personalizados de informações sensíveis, utilizando palavras chaves, expressões regulares e lógica booleana;

bn)A solução de SASE deve permitir a personalização de páginas HTML de bloqueio que são exibidas nos endpoints em certas situações com base nas configurações do Controle de Aplicação;

bo)A solução SASE deve permitir o login de usuários e aplicar políticas IAM para controle do acesso administrativo;

bp)A solução SASE deve implementar MFA para autenticação de usuários administrativos;

bq)A solução SASE deve manter em sua plataforma em nuvem as regras de segurança, seja para acesso à plataforma ou as políticas impostas pelo SASE, para controlar os usuários remotos. A plataforma de gerenciamento e configuração de políticas de segurança não deve ficar restrita a apenas um PoP e deve ser altamente disponível, replicando os perfis de segurança para todos os PoPs de segurança do cliente;

br)A solução SASE deve inspecionar a camada SSL/TLS durante a inspeção de certificados e as camadas superiores durante a inspeção profunda. A solução SASE deve filtrar e proteger o tráfego seguro que os vários perfis de segurança processaram. A inspeção SSL deve proteger, além do tráfego HTTPS, outros protocolos criptografados comumente usados, como SMTPS, POP3S, IMAPS e FTPS;

bs)A configuração do Secure Web Gateway da solução SASE deve ser feita sem a necessidade de um agente no endpoint para acesso HTTP e HTTPS, permitindo que políticas de segurança sejam aplicadas para proteger o acesso;

bt)O controle do CASB pode ser efetuado em console separada permitindo maior controle e segmentação de acesso através de perfis de IAM;

bu)O módulo CASB deve ter visibilidade de conteúdos do S3 Bucket da AWS, Storage do Azure e GCP, além das integrações do Microsoft e Google Workspace;

bv)Cada usuário deve ter direito de uso da solução em no mínimo 3 (três) dispositivos simultâneos.

6.4.1.6. CONTROLE DA REDE SEM FIO E COM FIO

a) Deve possuir funções de configuração WLAN e Switches a nível de: autenticação, criptografia, desempenho, inspeção de pacotes do tráfego local, detecção de aplicativos na rede, configuração de políticas e categorias de aplicativos, configurações dos rádios, otimização de canal, ajuste de potência de transmissão e ajuste de largura de canal de forma dinâmica;

b) A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada;

c) Deverá ser capaz de gerenciar, no mínimo, 256 APs;

d) Deverá ser capaz de gerenciar, no mínimo, 72 Switches.

6.4.1.7. FUNCIONALIDADE DE DETECÇÃO E PROTEÇÃO DE DISPOSITIVOS IOT

a) Deve ter a capacidade de identificar automaticamente o tipo de equipamento conectado (profiling), com suporte a dispositivos IoT (Internet of Things);

b) A identificação de dispositivos deve ser baseada em características do equipamento (Endereço MAC, Sistema Operacionais, entre outros) ou pelo usuário autenticado;

c) Deve permitir a identificação e mitigação de explorações de vulnerabilidades contra dispositivos IoT, realizando aplicações de patches;

d) A solução deve possuir uma base de dados de dispositivos IoT, atualizadas de forma regular e automática pelo fabricante da solução;

e) A solução deve ser capaz de identificar vulnerabilidades conhecidas em dispositivos IoT, fornecendo no mínimo os seguintes detalhes da vulnerabilidade encontrada: descrição, tipo, severidade, número do CVE e o link de referência do CVE.

6.4.1.8. FUNCIONALIDADE DE FILTRO DE DADOS - DLP

a) Permitir identificar e, opcionalmente, prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP);

b) Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

c) Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

d) Permitir identificar e, opcionalmente, prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;

e) Deve funcionar de maneira que consiga impedir que dados sensíveis saiam da rede e também deve funcionar de modo que se previna que dados não requisitados entrem na sua rede;

f) Deve possuir uma base de dados de dicionários e de padrões de dados pré-definidos, tais como números de cartões de crédito, trechos de código fonte de software, etc. Essa base deve ser atualizada de forma automática pelo FABRICANTE da solução;

g) Deve permitir especificar a informação sensível a ser detectada como palavras, frases e expressões regulares;

h) Deve permitir a criação e armazenamento de impressões digitais (fingerprint) de documentos;

i) Deve permitir a aplicação de regras baseadas em usuários autenticados, isto é, fazendo buscas pelo tráfego de um específico usuário autenticado;

j) Em tráfegos em que as regras definidas coincidirem, deve implementar no mínimo as seguintes ações: bloqueio, banimento e quarentena;

k) Deve armazenar, localmente ou na solução de gerenciamento centralizados de logs, o conteúdo do tráfego que coincidir com o tráfego esperado pela regra de DLP, em pelo menos os seguintes

protocolos: E-mail, HTTP e mensageiros instantâneos;

l) Deve permitir a composição de uma ou mais regras DLP, formando uma regra única mais específica que usa lógica booleana para fazer a comparação com o tráfego filtrado pelo sistema.

6.4.2. **WAF - Web Application Firewall - FortiWEB/FORTINET**

6.4.2.1. CARACTERÍSTICAS TÉCNICAS DA SOLUÇÃO

- a) Deve ser do tipo appliance virtual e recurso dedicado à função de Firewall de Aplicações WEB (WAF);
- b) Deve oferecer cluster de alta disponibilidade entre dois dispositivos no modo Ativo-Passivo e Ativo-Ativo, para que quando o principal falhar o tráfego possa continuar sendo processado;
- c) Deve possuir throughput mínimo para HTTP de 500 Mbps;
- d) Deve possuir throughput mínimo para HTTPS de 250 Mbps;
- e) Deve suportar, pelo menos 10 (dez) interfaces 1/10Gbps;
- f) Deve possuir suporte, no mínimo, a 4 (quatro) vCPUs;
- g) Deve suportar alocação de memória RAM ilimitada;
- h) Deve suportar armazenamento de, no mínimo, 2 (dois) TB;
- i) A máquina virtual deve suportar hipervisores como VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, VirtualBox, KVM disponibilizada pela contratante.

6.4.2.2. FUNCIONALIDADES DE REDE

- a) A solução deve ser capaz de ser implementada no modo proxy (Transparente e Reverso), passivo e inline transparente (Bridge);
- b) A solução deve ser capaz de ser implementada com protocolo WCCP;
- c) Suportar VLANs no padrão IEEE 802.1q;
- d) Deve implementar o protocolo de negociação Link Aggregation Control Protocol (LACP) - IEEE 802.3ad;
- e) Suportar endereçamento IPv4 e IPv6 nas interfaces físicas e virtuais (VLANs);
- f) A solução deve suportar e oferecer cluster de alta disponibilidade entre dois dispositivos no modo Ativo-Passivo e Ativo-Ativo, para que quando o principal falhar o tráfego possa continuar sendo processado;
- g) A solução deve suportar a sincronização de configuração entre dois appliances iguais, com o objetivo de operar no modo ativo-ativo, com a distribuição de tráfego sendo realizada por balanceador de carga externo ou pela própria solução;
- h) A solução deve suportar roteamento por política (policy route).

6.4.2.3. FUNCIONALIDADES DE GERÊNCIA

- a) O sistema operacional / firmware deve suportar interface gráfica web para a configuração das funções do sistema operacional, utilizando navegadores disponíveis gratuitamente e protocolo HTTPS, e através de CLI (interface de linha de comando), acessando localmente, via porta de console, ou remotamente via SSH;
- b) Deve possuir administração baseada em interface web HTTPS;
- c) Possuir auto-complementação de comandos na CLI;
- d) Possuir ajuda contextual na CLI;
- e) A solução deve possuir Interface Gráfica com informações sobre o sistema Ex: (Informações do Cluster, hostname, número de série, modo de operação, tempo em serviço, versão do firmware); Deverá ser possível visualizar através da interface gráfica de gerência informações de licenças e assinaturas;
- f) Deve prover, na interface de gerência, as seguintes informações do sistema para cada gateway: consumo de CPU e estatísticas das conexões;

- g) Deve ser possível visualizar na interface de gerência as informações de consumo de memória;
- h) Deve ser possível visualizar na interface de gerência ou CLI as informações de utilização de disco de log;
- i) Deverá possuir ferramenta, na interface gráfica de gerência (dashboard) que permita visualizar os últimos logs de ataque detectados/bloqueados;
- j) Deve prover as seguintes informações, na interface de gráfica de gerência: estatísticas de throughput HTTP em tempo real, estatísticas dos eventos de ataque detectados/bloqueados, estatísticas de requisições HTTP em tempo real e últimos logs de eventos do sistema;
- k) Possuir na interface gráfica estatísticas de conexões concorrentes e por segundo, de políticas de segurança do sistema;
- l) Possuir um painel de visualização com informações das interfaces de rede do sistema;
- m) A configuração de administração da solução deve possibilitar a utilização de perfis;
- n) Deve ser possível executar e restaurar backup via interface Web (GUI);
- o) Deve ter a opção para criptografar o backup;
- p) Deve ser possível executar e restaurar backup utilizando-se um ou mais dos seguintes protocolos: FTP, SFTP ou TFTP;
- q) Deve ser possível instalar um firmware alternativo em disco e inicializá-lo em caso de falha do firmware principal;
- r) Deve ter suporte ao protocolo de monitoração SNMP v1, SNMP v2c e SNMP v3;
- s) Deve ser capaz de realizar notificações de eventos de segurança através de e-mail, traps SNMP e Syslog;
- t) A solução deverá ter a capacidade de armazenar logs localmente em disco e em servidor externo via protocolo SYSLOG;
- u) Ter a capacidade de armazenar logs em appliance remoto;
- v) A solução deve ter a capacidade de enviar alertas por email de eventos baseados em severidades e/ou categorias;
- w) A solução deve possuir dados analíticos contendo localização geográfica dos clientes web;
- x) A solução deve possuir dados analíticos, sendo possível visualizar a contagem total de ataques e percentual de cada país de origem, o volume total de tráfego em bytes e percentual de cada país de origem e o total de acessos (hits) e percentual de cada país de origem;
- y) Deverá ter a capacidade de gerar relatórios detalhados baseados em tráfego/acessos/atividades do usuário;
- z) Deve ter suporte a RESTful API para gerenciamento de configurações.

6.4.2.4. FUNCIONALIDADES DE AUTENTICAÇÃO

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

6.4.2.5. ITENS REGULATÓRIOS E CERTIFICAÇÕES

- a) A solução deve suportar o modelo de segurança positiva definido pelo OWASP, pelo menos o que consta no TOP 10;

6.4.2.6. FUNCIONALIDADES DE WEB APPLICATION FIREWALL

- a) Deverá ser capaz de identificar e bloquear ataques através de um banco de dados de assinaturas de vírus e IP reputation, atualizado de forma automática;
- b) Deverá implementar recurso de machine learning, onde será permitido implementar proteção para um servidor ou grupo de servidores de aplicação web, de forma automatizada através da análise da utilização da aplicação, fazendo a descoberta da estrutura e padrões e padrões de uso, buscando separar o comportamento anormal do abusivo, detectando anomalias e tentativas de ataque;
- c) Ter a capacidade de criação de assinaturas de ataque customizáveis;
- d) Ter a capacidade de proteção para ataques do tipo Adobe Flash binary (AMF) protocol;
- e) Ter a capacidade de proteção para ataques do tipo Botnet;
- f) Ter a capacidade de proteção para ataques do tipo Browser Exploit Against SSL/TLS (BEAST);
- g) A solução deverá possuir funcionalidade de proteção positiva contra ataques como acesso por força bruta;
- h) Deve suportar detecção a ataques de Clickjacking;
- i) Deve suportar detecção a ataques de alteração de cookie;
- j) Identificar e prevenir ataques do tipo Credit Card Theft;
- k) Identificar e prevenir ataques Cross Site Request Forgery (CSRF);
- l) A solução deverá possuir funcionalidade de proteção positiva contra ataques como cross site scripting (XSS);
- m) Deve possuir proteção contra ataques de Denial of Service (DoS);
- n) Ter a capacidade de proteção para ataques do tipo HTTP header overflow;
- o) Ter a capacidade de proteção para ataques do tipo Local File inclusion (FLI);
- p) Ter a capacidade de proteção para ataques do tipo Man-in-the-middle (MITM);
- q) Ter a capacidade de proteção para ataques do tipo Remote File Inclusion (RFI);
- r) Ter a capacidade de proteção para ataques do tipo Server Information Leakage;
- s) Proteção contra envios de comandos SQL escondidos nas requisições enviadas a bases de dados (SQL Injection);
- t) Ter a capacidade de proteção para ataques do tipo Malformed XML;
- u) Identificar e prevenir ataques do tipo Low-rate DoS;
- v) Prevenção contra Slow POST attack;
- w) Proteger contra ataques Slowloris;
- x) Ter a capacidade de proteção para ataques do tipo SYN flood;
- y) Ter a capacidade de proteção para ataques do tipo Forms Tampering;
- z) A solução deverá possuir funcionalidade de proteção positiva contra ataques de manipulação de campo escondido;
- aa) Ter a capacidade de proteção para ataques do tipo Directory Traversal;
- ab) Ter a capacidade de proteção do tipo Access Rate Control;
- ac) Ter a habilidade de configurar proteção do tipo TCP SYN flood-style para prevenção de DoS para qualquer política, através de Syn Cookie e Half Open Threshold;
- ad) Permitir configurar regras de bloqueio a métodos HTTP indesejados;
- ae) Permitir que sejam configuradas regras de limite de upload por tamanho de arquivo;
- af) Deve permitir que o administrador bloqueie o tráfego de entrada e/ou tráfego de saída com base nos países, sem a necessidade de gerir manualmente os ranges de endereços IP correspondentes a cada país;
- ag) Deve suportar a criação de políticas por geolocalização, permitindo que o tráfego de determinado país seja bloqueado;

- ah) Permitir configurar listas negras de bloqueio e listas brancas de confiança, baseadas em endereço IP de origem;
- ai) Permitir a liberação temporária ou definitiva (whitelist) de endereços IP bloqueados por terem originados ataques detectados pela solução;
- aj) Deve permitir adicionar, automaticamente ou manualmente, em uma lista de bloqueio, os endereços IP de origem, de acordo com a base de IP Reputation;
- ak) Ter a capacidade de Prevenção ao Vazamento de Informações (DLP), bloqueando o vazamento de informações de cabeçalho HTTP;
- al) Ter a funcionalidade de proteger o website contra ações de desfiguração (defacement), com restauração automática e rápida do site caso ocorra à falha;
- am) Ter a funcionalidade de antivírus para inspeção de tráfego e arquivos;
- an) Ter a capacidade de investigar e analisar todo o tráfego HTTP para atestar se está em conformidade com a respectiva RFC, bloqueando ataques e tráfego em não-conformidade;
- ao) Deverá ser capaz de fazer aceleração de SSL, onde os certificados digitais são instalados na solução e as requisições HTTP são enviadas aos servidores sem criptografia;
- ap) A solução deve ser capaz de funcionar como Terminador de sessões SSL para a aceleração de tráfego;
- aq) Para SSL/TLS offload suportar no mínimo TLS 1.0; 1.1; 1.2 e 1.3;
- ar) A solução deve ter a capacidade de armazenar certificados digitais de CA's;
- as) A solução deve ser capaz de gerar CSR para ser assinado por uma CA;
- at) A solução deve conter as assinaturas de robôs conhecidos como link checkers, indexadores de web, search engines, spiders e web crawlers que podem ser colocados nos perfis de controle de acesso, bem como resetar tais conexões;
- au) Solução deve ter um sistema de reputação de endereços IP públicos conhecidos como fontes de ataques DDoS, botnets, spammers, etc. Tal sistema deve ser atualizado automaticamente;
- av) A solução deverá ser capaz de limitar o total de conexões permitidas para cada servidor real de um pool de servidores;
- aw) A solução deve permitir a customização ou redirecionar solicitações e respostas HTTP no HTTP Host, Request URL HTTP, HTTP Referer, HTTP Body e HTTP Location;
- ax) A solução deve permitir criar regras definindo a ordem em que as páginas devem ser acessadas para prevenir ataques como cross-site request forgery (CSRF);
- ay) A solução deve ter a capacidade de definir restrições a métodos HTTP;
- az) A solução deve ter a capacidade de proteger contra a detecção de campos ocultos;
- ba) Permitir que sejam criadas assinaturas customizadas de ataques e DLP, através de expressões regulares;
- bb) A solução deve incluir capacidade de atuar como um scanner de vulnerabilidades ou permitir a integração com scanners de vulnerabilidade de terceiros para diagnóstico e identificação de ameaças nos servidores web, software desatualizado e potenciais buffers overflows;
- bc) Deve gerar perfil de proteção automaticamente a partir de relatório em formato XML gerado por scanner de vulnerabilidade de terceiros;
- bd) A solução deve gerar um relatório da análise de vulnerabilidades no formato HTML;
- be) A solução deve permitir a exclusão de URLs na análise de vulnerabilidades;
- bf) Deverá ser capaz de fazer compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;
- bg) Suportar redireção e reescrita de requisições e respostas HTTP;
- bh) Permitir redirecionar requisições HTTP para HTTPS;
- bi) Permitir reescrever a linha URL no cabeçalho de uma requisição HTTP;
- bj) Permitir reescrever o campo "Host:" no cabeçalho de uma requisição HTTP;

- bk) Permitir reescrever o campo "Referer:" no cabeçalho de uma requisição HTTP;
- bl) Permitir redirecionar requisições para outro web site;
- bm) Permitir enviar resposta HTTP 403 Forbidden para requisições HTTP;
- bn) Permitir reescrever o parâmetro "Location:" no cabeçalho HTTP de uma resposta de redireção HTTP de um servidor web;
- bo) Permitir reescrever o corpo ("body") de uma resposta HTTP de um servidor web;
- bp) Permitir adicionar o campo X-Forwarded-For para identificação do endereço real do cliente quando no modo de proxy reverso;
- bq) A solução deve suportar regras para definir se as solicitações HTTP serão aceitas com base na URL e a origem do pedido e, se necessário, aplicar uma taxa específica de transferência (rate limit);
- br) A solução deve suportar o mecanismo de combinação de controle de acesso e autenticação utilizando mecanismos como HTML Form, Basic e Suporte a SSO, métodos como LDAP e RADIUS para consultas e integração dos usuários da aplicação;
- bs) Possuir capacidade de caching para aceleração web;
- bt) Deve permitir ao Administrador a criação de novas assinaturas e/ou alteração de assinaturas já existentes;

6.4.2.7.

FUNCIONALIDADES DE BALANCEAMENTO DE CARGA

- a) A solução deve incluir funcionalidade de balanceamento de carga entre servidores web;
- b) Deve ter a habilidade de configurar portas não-padrão para aplicação web HTTP e HTTPS;
- c) Ter a capacidade de balancear/distribuir tráfego e rotear o conteúdo através de vários servidores web;
- d) A solução deve permitir criar grupos de servidores (Server Farm / Pool) para distribuir as conexões dos usuários;
- e) Suportar algoritmo Round Robin para balanceamento de carga de servidores;
- f) Suportar algoritmo Weighted Round Robin para balanceamento de carga de servidores;
- g) Suportar algoritmo Least Connections para balanceamento de carga de servidores;
- h) A solução deve ser capaz de criar servidores virtuais que definem a interface de rede/bridge e endereço IP por onde o tráfego destinado ao Server Pool é recebido;
- i) Os servidores virtuais devem entregar o tráfego à um único servidor web e também possuir a opção de distribuir as sessões/conexões entre os servidores web do Server Pool;
- j) Deve ser possível especificar o número máximo de conexões TCP simultâneas para um determinado servidor membro do Server Pool;
- k) Permitir teste de disponibilidade de servidor web através do método TCP;
- l) Permitir teste de disponibilidade de servidor web através do método ICMP ECHO_REQUEST (ping);
- m) Permitir teste de disponibilidade de servidor web através do método TCP Half Open;
- n) Permitir teste de disponibilidade de servidor web através do método TCP SSL;
- o) Permitir teste de disponibilidade de servidor web através do método HTTP;
- p) Permitir teste de disponibilidade de servidor web através do método HTTPS;
- q) Nos testes de disponibilidade HTTP e HTTPS, permitir indicar a URL exata a ser testada;
- r) Nos testes de disponibilidade HTTP e HTTPS, permitir escolher entre os métodos HEAD, GET e POST;
- s) Nos testes de disponibilidade HTTP e HTTPS, permitir indicar o nome do campo HTTP "host" a ser testado;
- t) Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Host";

- u) Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de “URL”;
- v) Suportar roteamento das requisições dos clientes web baseado “Parâmetro HTTP”;
- w) Suportar roteamento das requisições dos clientes web baseado “Referer”;
- x) Suportar roteamento das requisições dos clientes web baseado “Endereço IP de Origem”;
- y) Suportar roteamento das requisições dos clientes web baseado “Cabeçalho”;
- z) Suportar roteamento das requisições dos clientes web baseado “Cookie”;
- aa) Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de “Valor de campo do Certificado X509”;
- ab) Implementar Cache de Conteúdo para HTTP, permitindo que objetos sejam armazenados e requisições HTTP sejam respondidas diretamente pela solução;
- ac) A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por endereço IP de origem;
- ad) A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência analisando qualquer parâmetro do header HTTP;
- ae) A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência analisando a URL acessada;
- af) A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existente no mesmo servidor, implementando persistência por cookie – método cookie insert e cookie rewrite;
- ag) A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por embedded cookie (cookie original mais porção randômica);
- ah) A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em Reescrita de Cookie;
- ai) A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em Cookie Persistente;
- aj) A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em ASP Session ID;
- ak) A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em PHP Session ID;
- al) A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em JSP Session ID;
- am) A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por sessão SSL.

6.4.2.8. FUNCIONALIDADES DE PROTEÇÃO API

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

- h) Permitir definir elementos proibidos XML tais como entidade externa, XInclude, local do esquema, entre outros;
- i) Permitir definir o seguinte formato do esquema: SOAP ou XML;
- j) Permitir definir o nível de severidade dos logs das ações;
- k) Fornecer suporte à proteção OpenAPI;
- l) Permitir o upload de arquivo de descrição OpenAPI, e bloquear as solicitações que não correspondam às definições do arquivo;
- m) Suportar a proteção de API Movel;
- n) Permitir a verificação de flags de API móvel e com a regra de proteção de API configuradas, executar as ações definidas na regra de proteção;
- o) Permitir definir o nível de severidade dos logs das ações;
- p) Suportar as seguintes funções de API gateway:
- q) Gerenciamento de usuários API

- Verificação de chave API

- Controle de acesso API

- Controle de limite de taxa

- Reescrita de chamada de API

- Permitir definir usuários de API para restringir o acesso a APIs com base em chaves de API.

- Permitir a restrição baseada em endereçamento IP

- Permitir a restrição baseada em referenciadores HTTP

- Permitir a criação de grupos de usuários.

- Permitir restringir o acesso à API através de regras envolvendo verificação de chave API, transferência de chave API, agrupamento de usuários API, configuração de sub-URL e ações específicas de qualquer violação de chamada API.

6.5. SERVIÇOS DE SUPORTE E MANUTENÇÃO - LOTES I, II E III:

6.5.1. O SLA para os serviços será de acordo com a Tabela, sendo que a "Classe de Serviço A," refere-se ao circuito de dados para conexão do datacenter e do contêiner a rede mundial de computadores.

6.5.2. Deverão ser utilizados enlaces de comunicação terrestre por fibra óptica, sem prejuízo dos prazos de implantação, restrições e critérios de desempenho estabelecidos nesta especificação, deve, obrigatoriamente, utilizar as seguintes tecnologias: ATM ou Ethernet/Metro Ethernet, suportando o protocolo TCP/IP, com acessos de última milha terrestre, garantindo a banda mínima necessária.

Requisitos mínimos obrigatórios (por link)	Referência	Lotes
Velocidade do Link - Especifica a velocidade tanto de download quanto de upload (Link Full)	5Gbps	I e II
Tipo de acesso - Especifica o tipo de acesso - Especifica o tipo de conexão da unidade remota do órgão	Internet com acesso terrestre	I e II
Disponibilidade de Serviço - Relação entre o tempo de operação plena e prejudicada no período 30 (trinta) dias	99,35%	I e II
Tempo máximo de retardo admissível - o tempo máximo de retado na comunicação unilateral entre o ponto de conexão e o roteador de borda da	Deverá ser igual ou inferior a 65 ms	I e II

proponente para um pacote de 32 Bytes		
Banda mínima garantida – banda mínima disponível para acesso a internet para cada um dos pontos contemplados	100% da largura de Banda Contratada	I e II
Taxa de perda de pacote - taxa máxima admissível de perda de pacote	1%	I e II
Ativação – período entre a solicitação e ativação do serviço	45 (quarenta e cinco) dias	I, II e III
Prazo de resposta - período máximo para o deslocamento de técnico da contratada até o endereço associado à reclamação de suporte (se necessário o deslocamento)	2 (duas) horas	I, II e III
Prazo de solução - período máximo para o restabelecimento do serviço, contado a partir do momento da abertura do chamado até a finalização do atendimento	4 (quatro) horas	I, II e III
Prazo mínimo de notificação de manutenção preventiva ou atualização de recursos técnicos – período mínimo entre a notificação do cliente pela operadora até o início da interrupção	7 (sete) dias	I, II e III
Abertura de chamado - disponibilidade de atendimento para solicitações de reparos, help-desk da operadora contratada e discagem sem cobrança (0800) em língua portuguesa	24x7	I, II e III
Horário de reparo - disponibilidade de atendimento técnico a partir da abertura do chamado	24x7	I, II e III
Quantidade mínima de endereços IP disponíveis	64	I e II

6.5.3. Observações:

- a) LOTES I e II - **Link dedicado de acesso a internet e Serviço de mitigação de ataques de negação de serviço (DDOS);**
- b) LOTE III - **Solução de segurança de perímetro.**

6.5.3.1. GERENCIAMENTO DOS SERVIÇOS

I - A CONTRATADA deverá prover um serviço de gerenciamento, a partir do seu próprio CGR – Centro de Gerência de Rede, que deverá apresentar pelo menos as seguintes características de atendimento:

- a) Regime de trabalho 24 x 7 x 365;
- b) Acesso por Discagem Direta Gratuita (DDG – 0800);
- c) Abertura de chamados para intervenção técnica de forma proativa e reativa;
- d) Nas ocorrências detectadas pelo Sistema de Gerência de Falhas (SGF), os analistas contatarão, pro-ativamente, o responsável no CONTRATANTE, fornecendo informações precisas sobre a interrupção no serviço detectada;
- e) Os analistas do CGR farão a abertura do chamado para acionamento da área técnica de forma que esta última possa intervir no caso e restabelecer o serviço nas condições contratadas;
- f) A CONTRATADA deve disponibilizar pelo menos um Centro Operacional de Segurança (ou SOC – Security Operations Center) no Brasil, com equipe especializada em monitoramento,

detecção e mitigação de ataques, com opção de atendimento através de telefone 0800, correio eletrônico, em idioma português brasileiro, durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual.

6.5.3.2. MONITORAMENTO DOS SERVIÇOS

I - A CONTRATADA deve disponibilizar as seguintes informações acerca dos acessos da rede:

- a) Status instantâneo de cada acesso (ativo/inativo) e o tempo decorrido desde a última mudança de status. Deverá ser disponibilizada uma visão diagramada de toda a rede (topologia da rede com informações dos serviços contratados) num display instalado no CONTRATANTE ou por meio de uma página WEB disponível na Intranet e/ou Internet com acesso controlado por senha a ser disponibilizada pela CONTRATADA;
- b) Ocupação da banda total do acesso e da banda disponibilizada para cada Classe de Serviço configurada para cada acesso;
- c) Taxa de erro ou perda de pacotes em cada acesso;
- d) Ocupação do processador e da memória de cada roteador;
- e) Inventário dos equipamentos e enlaces da rede contendo, no mínimo, as seguintes informações:
- f) Enlace: designação, tecnologia e nível de serviço;
- g) Roteador CPE: fabricante e modelo, configuração lógica e configuração físicas (placas, interfaces, memória, slots, dentre outros);
- h) Endereçamento lógico: endereços IPs e máscaras;
- i) Geração de relatórios consolidados com informação do histórico de chamados técnicos de cada acesso com a data e horário da abertura e do encerramento, tempo para a recuperação do serviço e causa da ocorrência;
- j) A Solução de Gerenciamento e Monitoração da Rede deverá realizar registro de todas as ocorrências de alarmes/eventos em log de históricos e/ou em base de dados contendo informações de data e hora de ocorrência, identificando os recursos gerenciados.

7. DA NATUREZA DA CONTRATAÇÃO E ALINHAMENTO ESTRATÉGICO

7.1. Caracterização do Objeto

7.1.1. O objeto desta contratação consiste em uma solução integrada de Tecnologia da Informação e Comunicação (TIC), estruturada para garantir a conectividade, a continuidade e a segurança dos sistemas da SEFAZ/AC. Trata-se de uma solução descrita de forma objetiva, clara e suficiente, de modo a evitar dúvidas sobre as especificações técnicas e operacionais exigidas.

7.1.2. Dada a sua natureza essencial para o funcionamento ininterrupto da infraestrutura tecnológica da SEFAZ/AC, o objeto enquadra-se como **serviços e fornecimentos contínuos**, nos termos do inciso XV do art. 6º da Lei nº 14.133/2021, conforme transcrição:

“Art. 6º Para os fins desta Lei, consideram-se:

(...)

*XV – **serviços e fornecimentos contínuos**: serviços contratados e compras realizadas pela Administração Pública para a manutenção da atividade administrativa, decorrentes de necessidades permanentes ou prolongadas.*

7.2. Alinhamento Estratégico

7.2.1. A presente contratação está alinhada com os objetivos estratégicos da instituição, que incluem a busca contínua pela excelência na gestão pública, a transparência nas contratações e a promoção da inovação e, tem como base o alinhamento à missão, o Planejamento Estratégico e o Plano Diretor de Tecnologia da Informação (PDTI), atendendo aos seguintes objetivos estratégicos

- **OE3** – Acelerar a transformação digital de forma sistêmica, aprimorando a gestão de Tecnologia da Informação;
- **OE6** – Otimizar as infraestruturas de TI;
- **OE9** – Garantir a gestão eficiente dos recursos orçamentários e financeiros de TI.

8. DA FUNDAMENTAÇÃO DA CONTRATAÇÃO

8.1. Da Referência ao Estudo Técnico Preliminar e no Plano de Contratação Anual

8.1.1. A contratação encontra-se contemplada no Plano de Contratação Anual da Secretaria de Estado da Fazenda (SEI nº 0715.012462.00176/2024-88) para o ano corrente, conforme previsto no **item 3.6 - SERVIÇOS DE TIC - Links de acesso à INTERNET**.

8.2. Demais normativos que fundamentam a contratação:

- Lei nº 14.133, de 1º de abril de 2021 - Regulamento Lei de Licitações e Contratos Administrativos.
- Decreto Estadual nº 11.363, de 22 de novembro de 2023 – que regulamenta a Lei nº 14.133/2021, no âmbito do Estado do Acre.

9. DO PARCELAMENTO DO OBJETO

9.1. O objeto em questão caracteriza-se como uma **Solução de Tecnologia da Informação e Comunicação (TIC)**, conforme diretrizes da Instrução Normativa SEGES/ME nº 1/2019 e demais normativos correlatos, por se tratar de um conjunto de bens e serviços integrados que apoiam os processos de negócio da SEFAZ/AC, assegurando desempenho, continuidade e proteção dos serviços digitais essenciais à gestão fiscal e financeira do Estado.

9.2. A Lei 14.133/2021, em seus **art. 40, inciso V, alínea ‘b’, §§ 2º, inciso I**, determina que o parcelamento do objeto deve ser adotado quando tecnicamente viável e economicamente vantajoso. Entretanto, a mesma legislação prevê exceções, **admitindo a contratação em LOTE quando o objeto for tecnicamente integrado, a divisão comprometer a economia de escala, aumentar custos de gestão, ou houver risco à funcionalidade do sistema como um todo**. Senão vejamos:

"Art. 40. O planejamento de compras deverá considerar a expectativa de consumo anual e observar o seguinte:

(...)

V - atendimento aos princípios:

(...)

b) do parcelamento, quando for tecnicamente viável e economicamente vantajoso;

(...)

§ 2º Na aplicação do princípio do parcelamento, referente às compras, deverão ser considerados:

I - a viabilidade da divisão do objeto em lotes;

(...)

§ 3º O parcelamento não será adotado quando:

(...)

II - o objeto a ser contratado configurar sistema único e integrado e houver a possibilidade de risco ao conjunto do objeto pretendido;

(...)

"Art. 47. As licitações de serviços atenderão aos princípios:

(...)

II - do parcelamento, quando for tecnicamente viável e economicamente vantajoso." (Grifamos)

9.3. A divisão em três lotes foi definida com base em critérios técnicos, funcionais e de segurança. Os LOTES I e II tratam da conectividade principal e redundante, que devem **obrigatoriamente ser fornecidos por empresas distintas** para garantir a continuidade dos serviços críticos. Já o **LOTE III**, embora independente tecnicamente, é complementar e fundamental à solução como um todo, por oferecer a proteção de perímetro e aplicação que preserva o ambiente contra ameaças externas, **garantindo segurança integrada aos dados** e serviços públicos prestados pela SEFAZ/AC.

9.4. Os lotes estão estruturados da seguinte forma:

I - **LOTE I** – *Link dedicado de acesso à internet (5 Gbps) + Serviço de mitigação de ataques DDoS*: Representa o link principal da SEFAZ/AC, responsável por assegurar a operação dos sistemas fazendários e plataformas acessadas por contribuintes, servidores e outros órgãos públicos. A mitigação de ataques DDoS é essencial para garantir alta disponibilidade, estabilidade e continuidade dos serviços digitais.

II - **LOTE II** – *Link dedicado de acesso à internet (5 Gbps - Redundância) + Serviço de mitigação de ataques DDoS*: Corresponde à infraestrutura de backup e contingência, sendo vital para a redundância lógica e física da conectividade institucional. Em caso de falha ou

indisponibilidade do link principal, este enlace assume automaticamente as funções de acesso, assegurando a continuidade dos serviços críticos.

III - **LOTE III – Solução de segurança de perímetro e Web Application Firewall (WAF):** Trata-se de uma solução especializada para proteção de rede, com cluster de alta disponibilidade, que atua como barreira contra ameaças externas e vulnerabilidades nas aplicações web. O WAF é essencial para garantir a integridade, confidencialidade e disponibilidade dos dados e sistemas estratégicos da SEFAZ/AC. Essa solução assegura a confidencialidade, integridade e disponibilidade das informações e sistemas da SEFAZ/AC.

9.5. Por razões técnicas e de segurança, **a mesma empresa não poderá ser adjudicatária simultaneamente dos LOTES I e II**, ainda que apresente a melhor proposta em ambos. **Essa exigência visa garantir a redundância efetiva** da solução de conectividade, reduzindo os riscos de indisponibilidade por falha técnica, contratual ou estrutural do fornecedor. A contratação de empresas distintas mitiga o risco de ponto único de falha e reforça a resiliência da infraestrutura de rede da SEFAZ/AC.

9.6. Por fim, a opção pelo **parcelamento do objeto** em lotes está plenamente alinhada aos princípios e fundamentos legais da **Lei nº 14.133/2021**, especialmente ao art. 40, § 2º, promovendo uma contratação racional, eficiente e segura para o interesse público que todos os equipamentos e serviços listados constituem partes integradas de uma solução única em cada lote, é tecnicamente imprescindível sua contratação em **LOTES**. Essa medida visa garantir a total interoperabilidade e compatibilidade entre os dispositivos, a eficiência do processo de implementação e a concentração da responsabilidade na entrega, mitigando riscos de falhas de integração e facilitando o suporte, a manutenção e o gerenciamento centralizado da infraestrutura instalada. A presente justificativa está amparada no art. 18, §1º, inciso VIII, combinado com o art. 40, V, "a", § 2º I e § 3º I e II, da Lei nº 14.133/2021.

10. OUTROS REQUISITOS DA CONTRATAÇÃO

10.1. Subcontratação

10.1.1. Não será admitida a subcontratação do objeto a ser contratado.

10.2. Garantia de Execução Contratual

10.2.1. No ato da assinatura do Contrato, o fornecedor deve apresentar comprovante de garantia para sua execução, com validade durante todo período de vigência contratual, correspondente a 5% (cinco por cento) de seu valor global, em uma das modalidades de garantia previstas no art. 96 da Lei 14.133/21:

- I - Caução em dinheiro ou em títulos da dívida pública;
- II - Seguro garantia;
- III - Fiança bancária.
- IV - Título de Capitalização.

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

- a) Prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;
- b) Prejuízos causados à Administração ou a terceiro, decorrentes de culpa ou dolo durante a execução do contrato;
- c) Multas moratórias e punitivas aplicadas pela Administração ao contratado; e
- d) Obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza, não adimplidas pelo contratado.

10.2.3. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso, observado o máximo de 2% (dois por cento).

10.2.4. O garantidor não é parte interessada para figurar em processo administrativo instaurado pela contratante com o objetivo de apurar prejuízos e/ou aplicar sanções ao contratado.

10.2.5. A garantia será considerada extinta com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da Administração, mediante termo circunstanciado, de que a CONTRATADA cumpriu todas as cláusulas do contrato.

10.2.6. A garantia prestada deverá vigorar por mais 90 (noventa) dias após o término da vigência contratual e será liberada ou restituída a CONTRATADA findo este prazo, desde que integralmente cumpridas todas as obrigações

assumidas, inclusive as trabalhistas. Caso o pagamento das verbas rescisórias trabalhistas não ocorra até o fim do segundo mês após o encerramento da vigência contratual, a garantia será utilizada para o pagamento dessas verbas diretamente pela Contratante;

10.2.7. A Contratante não executará a garantia nas seguintes hipóteses:

- a) Caso fortuito ou força maior;
- b) Alteração, sem prévia anuência da seguradora ou do fiador, das obrigações contratuais;
- c) Descumprimento das obrigações pelo contratado decorrente de atos ou fatos da Administração;
- d) Prática de atos ilícitos dolosos por servidores da Administração;

10.2.8. Não serão admitidas outras hipóteses de não execução da garantia, que não as previstas no item anterior;

10.2.9. Cabe à própria administração apurar a isenção da responsabilidade prevista nos incisos III e IV acima, não sendo a entidade garantidora parte no processo instaurado pela CONTRATANTE;

10.2.10. A CONTRATADA se compromete a repor ou a completar a garantia na hipótese de utilização parcial ou total, inclusive na hipótese de utilização para indenização a terceiros, e, ainda, na alteração do valor contratado, para manter o percentual inicial, no prazo de 48 (quarenta e oito) horas, a partir da data em que for notificada pela Contratante, mediante correspondência entregue contra recibo.

10.3. **Requisitos de Segurança e Privacidade**

10.3.1. A CONTRATADA deve seguir as orientações de segurança da SEFAZ/AC e legislação pertinente ao assunto, bem como:

- a) Submeter-se aos procedimentos contidos nas normas de segurança corporativa do órgão em todos os eventos em que for necessária a presença de seus prepostos e/ou funcionários nas dependências da CONTRATANTE, inclusive durante o período de prestação dos serviços de garantia.
- b) Exigir dos seus empregados, quando em serviço nas dependências da CONTRATANTE, o uso obrigatório de uniformes e crachás de identificação.
- c) Não poderá se utilizar da presente contratação para obter qualquer acesso não autorizado as informações de propriedade da CONTRATANTE.
- d) Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de que tomar conhecimento em razão da execução do objeto do contrato, respeitando todos os critérios de sigilo, segurança e inviolabilidade, aplicáveis aos dados, informações, regras de negócio, documentos, entre outros.
- e) Deverá assinar os Termos de Compromisso do Sigilo e Confidencialidade, e seus funcionários alocados na prestação de serviços o Termo de Ciência, conforme modelos anexos ao Termo de Referência.
- f) Deverá comunicar imediatamente a CONTRATANTE qualquer ocorrência de transferência, remanejamento ou demissão de funcionários envolvidos diretamente na execução do objeto, para que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e recursos do CONTRATANTE, porventura colocados à disposição para realização dos serviços contratados.

10.4. **Requisitos Documentais**

10.4.1. A contratada deverá apresentar todos os documentos exigidos pela Lei 14.133/2021, incluindo a documentação fiscal regularizada, inscrição no CNPJ, certidões negativas de débitos e comprovação de regularidade com a Seguridade Social e o Fundo de Garantia por Tempo de Serviço (FGTS).

10.4.2. As comprovações das características técnicas solicitadas no termo de referência devem ser claras, através do fornecimento de documentos cuja origem seja exclusivamente do fabricante dos produtos, como: catálogos, manuais, ficha de especificação técnica, informações obtidas em sites oficiais do fabricante através da internet, indicando as respectivas URL (Uniform Resource Locator).

10.4.2.1. A não comprovação de algum parâmetro solicitado pela CONTRATANTE, levará a desclassificação da proposta.

10.4.2.2. Apresentação das comprovações características técnicas devem ser submetidos a avaliação técnica pelo Departamento de Tecnologia da Informação desta SEFAZ/AC.

10.5. Requisitos Legais

10.5.1. O presente processo de contratação tem como fundamentação básica à:

- a) Constituição da República Federativa do Brasil;
- b) Lei nº 14.133/21, (Lei de Licitações e Contratos Administrativos);
- c) Decreto nº 11.462, de 31 de março de 2023; Decreto nº 11.363, de 22 de novembro de 2023; e
- d) Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022.

10.6. Amostra

10.6.1. Não será exigida a apresentação de amostras.

10.7. Vistoria

10.7.1. Para o correto dimensionamento e elaboração de sua proposta, será facultado à LICITANTE realizar vistoria para conhecer a infraestrutura e as instalações do CONTRATANTE.

10.7.2. O prazo para vistoria iniciar-se-á no dia útil seguinte ao da publicação do Edital, estendendo até 5 (cinco) dias corridos antes da data marcada para o recebimento de propostas.

10.7.2.1. O licitante que optar por realizar vistoria prévia terá disponibilizado pela Administração data e horário exclusivos, a ser agendado junto ao Departamento de Tecnologia da Informação - DETI, por meio do telefone (68) 3212-7958 ou pelo E-mail: deti@sefaz.ac.gov.br, em dias úteis, das 8h às 14h, de modo que seu agendamento não coincida com o agendamento de outros licitantes.

10.7.2.2. A visita destina-se à vistoria preliminar, avaliação e ciência das empresas interessadas para conhecimento pleno das condições e peculiaridades do objeto a ser contratado, com fins de elaboração da proposta e demais efeitos decorrentes deste Edital.

10.7.2.3. A vistoria deverá ser feita por profissional qualificado da empresa interessada, o qual deverá estar munido de documento de identificação e de instrumento que o habilite à representação legal da empresa.

10.7.3. Para todos os efeitos, considerar-se-á que a LICITANTE, optante pela realização de vistoria ou não, tem pleno conhecimento da natureza e do escopo dos serviços, não se admitindo, posteriormente, qualquer alegação de desconhecimento dos serviços e de dificuldades técnicas não previstas.

10.7.4. Efetuada a vistoria será lavrado, por representante da equipe técnica, designado para tanto, o respectivo termo conforme ANEXO II - DECLARAÇÃO DE VISTORIA, o qual deverá ser preenchido e assinado pelo interessado em participar da licitação, anexando à sua habilitação.

10.7.5. A não realização da vistoria, não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo a licitante vencedora assumir os ônus dos serviços decorrentes.

10.7.6. Caso a LICITANTE renuncie à vistoria técnica, deverá entregar o respectivo termo conforme ANEXO III - DECLARAÇÃO DE RENÚNCIA À VISTORIA TÉCNICA, o qual deverá ser preenchido e assinado pelo interessado em participar da licitação, anexando à sua habilitação.

10.8. Requisitos Sociais, Ambientais e culturais

10.8.1. A CONTRATADA deverá cumprir, no que couber, as exigências do inciso XI, art. 7º da Lei nº 12.305, de 02 de agosto de 2010, que institui a Política Nacional de Resíduos Sólidos – PNRS.

“XI - prioridade, nas aquisições e contratações governamentais, para:

(...)

b) bens, serviços e obras que considerem critérios compatíveis com padrões de consumo social e ambientalmente sustentáveis;” (Grifamos)

11. DO PRAZO DA CONTRATAÇÃO

11.1. Da Assinatura do Contrato

11.1.1. O prazo para assinatura do Contrato por parte do licitante vencedor será de 10 (dez) dias corridos, contados a partir da notificação feita pela SEFAZ/AC, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas em Lei.

11.1.2. O prazo de convocação poderá ser prorrogado 1 (uma) vez, por igual período, mediante solicitação da parte durante seu transcurso, devidamente justificada, e desde que o motivo apresentado seja aceito pela Administração.

11.2. Da Vigência Contratual

11.2.1. O prazo de vigência da contratação é de **60 (sessenta) meses** contados da data da assinatura do contrato, prorrogável na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021, vejamos:

"Art. 106. A Administração poderá celebrar contratos com prazo de até 5 (cinco) anos nas hipóteses de serviços e fornecimentos contínuos, observadas as seguintes diretrizes:

I - a autoridade competente do órgão ou entidade contratante deverá atestar a maior vantagem econômica vislumbrada em razão da contratação plurianual;

II - a Administração deverá atestar, no início da contratação e de cada exercício, a existência de créditos orçamentários vinculados à contratação e a vantagem em sua manutenção;

III - a Administração terá a opção de extinguir o contrato, sem ônus, quando não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

§ 1º A extinção mencionada no inciso III do caput deste artigo ocorrerá apenas na próxima data de aniversário do contrato e não poderá ocorrer em prazo inferior a 2 (dois) meses, contado da referida data.

§ 2º Aplica-se o disposto neste artigo ao aluguel de equipamentos e à utilização de programas de informática.

Art. 107. Os contratos de serviços e fornecimentos contínuos poderão ser prorrogados sucessivamente, respeitada a vigência máxima decenal, desde que haja previsão em edital e que a autoridade competente ateste que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o contratado ou a extinção contratual sem ônus para qualquer das partes."

11.2.2. Da Eficácia

11.2.3. A eficácia do contrato estará condicionada à publicação do extrato no Diário Oficial do Estado do Acre e no Portal Nacional de Contratações Públicas (PNCP).

11.2.4. A divulgação no Portal Nacional de Contratações Públicas (PNCP), de acordo com o art. 94, inciso II, da Lei nº 14.133/21, é condição indispensável para a eficácia do contrato e de seus aditamentos e, no caso de licitação deverá ocorrer em até 20 (vinte) dias úteis contados da data de sua assinatura.

12. DO MODELO DE EXECUÇÃO DO OBJETO

12.1. Início da Execução do Objeto

12.1.1. A Empresa CONTRATADA deverá entregar o objeto no prazo máximo de até 60 (sessenta) dias corridos, a contar da data do recebimento da ordem de serviço, com possibilidade de dilação do prazo por igual período desde que formalizado pela CONTRATADA

12.1.2. O objeto deste contrato será recebido da seguinte forma:

a) Provisoriamente, em até 5 (cinco) dias corridos, após a entrega, para efeito de posterior verificação da conformidade dos itens com as especificações deste Termo de Referência.

b) Definitivamente, em até 10 (dez) dias após o recebimento provisório, mediante atesto na nota fiscal/fatura, após a verificação da qualidade dos serviços e aceitação pelo fiscal deste instrumento convocatório.

12.1.3. Não serão admitidos para efeito de recebimento itens que estejam em desacordo ou conflitantes com quaisquer especificações prescritas neste Termo de Referência.

12.1.4. O recebimento do objeto desta contratação será condicionado à conferência, ao exame qualitativo e à aceitação final, obrigando-se a CONTRATADA a reparar, corrigir, substituir, no todo ou em parte, sanar os vícios, defeitos ou as incorreções porventura detectadas.

12.1.5. O recebimento dar-se-á por meio de Termo de Aceite, emitido pelo Departamento de Tecnologia da Informação da CONTRATANTE, provisoriamente em até 5 (cinco) dias corridos, contados da ativação do mesmo e de forma definitiva em até 10 (dez) dias corridos do recebimento provisório, após verificado o perfeito estado de funcionamento e atendimento às características exigidas neste documento e anexos.

12.1.6. O faturamento de cada acesso terá início a partir da data da emissão do Termo de Aceite.

12.1.7. Em caso de falta de manifestação por parte da CONTRATANTE o serviço será automaticamente considerado aceito de forma automática após 15 (quinze) dias corridos da ativação dos serviços.

12.1.8. Local e Serviço de Instalação

12.1.8.1. Os equipamentos fornecidos para a execução dos serviços deverão ser entregues no Departamento de Tecnologia da Informação da SEFAZ/AC, situado à Rua Benjamin Constant, 946 – Centro, Rio Branco – AC, 69900-062.

12.1.8.2. Os equipamentos deverão ser instalados no Datacenter da Contratante, em substituição aos equipamentos lá existentes - utilizando a mesma estrutura elétrica e espaço físico, considerando instalação lado a lado ou “side to side”.

12.1.8.3. Toda a instalação deverá ocorrer com agendamento prévio e acompanhamento de técnico indicado pelo SEFAZ - AC.

12.1.8.4. O cabeamento para conexão dos equipamentos, bem como os conectores e acessórios necessários para a montagem deverão ser fornecidos pela CONTRATADA.

12.1.8.5. Fazem parte da instalação todas as conexões e configurações necessárias para o funcionamento do objeto.

12.2. **Garantia**

12.2.1. A CONTRATADA deverá prestar serviços de garantia dos itens que compõe o objeto que encontram-se pormenorizadas no **item 6 - Especificações Técnicas Mínimas**, durante a vigência do contrato.

12.2.2. A CONTRATADA deverá fornecer todos os equipamentos necessários ao funcionamento dos serviços, bem como a instalação, garantia de peças, suporte e assistência técnica permanente dos equipamentos, objetivando atender necessidade atual de comunicação, com manutenção e reposição de partes e peças desgastadas pelo uso normal do equipamento.

12.2.3. A CONTRATADA aplicará nos equipamentos, quando necessário, a substituição de partes e peças originais, novas ou, quando não, que mantenham as especificações técnicas do fabricante, ficando desde logo, autorizada pela SEFAZ/AC.

12.2.4. Todos os serviços de manutenção devem ser efetuados, conforme definido neste Termo, desde o início até o final do contrato. São de inteira responsabilidade da CONTRATADA, e devem estar totalmente cobertos pelo pagamento mensal relativo ao fornecimento dos serviços, sem que isso implique acréscimos nos preços contratados.

12.2.5. Os serviços de manutenção devem cobrir todas as despesas relacionadas com a troca ou reposição de peças, manutenção de softwares e reparos de instalações, incluindo as despesas de deslocamento de técnicos, diárias, hospedagem e demais gastos relacionados com a equipe técnica de manutenção.

12.2.6. **Manutenção e Suporte Técnico**

12.2.7. A CONTRATADA deverá prestar os serviços em conformidade com as especificações contidas no item 6 - Termo de Referência e em sua Proposta, sem defeitos ou avarias, sendo aplicadas todas as normas e exigências do Código de Defesa do Consumidor (art. 39, VIII, da Lei nº 8.078/90) e demais legislação aplicáveis à espécie.

12.2.8. A contratada é a responsável pela identificação e resolução dos problemas que afetem o desempenho e a operacionalidade dos serviços contratados.

12.2.9. Efetuar manutenção preventiva na solução, de forma a identificar possíveis pontos de falha e garantir o perfeito funcionamento de todos os serviços.

12.2.10. Efetuar manutenção corretiva assim que for detectado algum mau funcionamento em equipamentos, ou problemas em instalações feitas, de forma que voltem a funcionar perfeitamente.

12.2.11. O serviço de manutenção corretiva deve incluir o reparo e a substituição de peças defeituosas em equipamentos que compõe o objeto.

12.2.12. Realizar o serviço de manutenção no local de instalação do equipamento sempre que possível. Caso seja necessário remover o equipamento, a CONTRATADA deve providenciar a substituição do equipamento que compõe o objeto por outro idêntico em perfeito funcionamento, para então retirar o equipamento com defeito e encaminhá-lo para a manutenção.

13. **DAS OBRIGAÇÕES DA CONTRATANTE**

13.1. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta.

13.2. Encaminhar formalmente as demandas de acordo com os critérios constantes deste Termo de Referência.

- 13.3. Exercer o acompanhamento e a fiscalização do(s) contrato(s) por intermédio de servidores especialmente designados, na forma prevista no art. 140 da Lei nº 14.133/2021.
- 13.4. Notificar a CONTRATADA através de e-mail, de ocorrência de eventuais imperfeições, falhas ou irregularidades no curso da execução dos serviços, para que sejam adotadas as medidas corretivas necessárias.
- 13.5. Efetuar o pagamento à CONTRATADA no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Contrato e seus anexos.
- 13.6. Aplicar à CONTRATADA as sanções administrativas regulamentares e contratuais cabíveis.
- 13.7. Notificar a CONTRATADA, por escrito, de eventuais aplicações de multas, previstas no contrato.
- 13.8. Exigir o fiel cumprimento de todos os compromissos assumidos pela CONTRATADA.
- 13.9. A CONTRATANTE não responderá por quaisquer compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução do presente contrato, bem como por quaisquer danos causados a terceiros em decorrência de ato da CONTRATADA e de seus empregados, prepostos ou subordinados.

14. DAS OBRIGAÇÕES DA CONTRATADA

- 14.1. Executar a entrega dos serviços conforme especificações deste Termo de Referência e de sua proposta, na qualidade e quantidade especificadas.
- 14.2. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo Gestor do contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados.
- 14.3. Reparar quaisquer danos diretamente causados à SEFAZ ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou acompanhamento da execução dos serviços pela SEFAZ.
- 14.4. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com os artigos 12 a 14 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990), ficando a SEFAZ autorizada a descontar da garantia, caso exigida no edital, ou dos pagamentos devidos à CONTRATADA, o valor correspondente aos danos sofridos.
- 14.5. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.
- 14.6. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato.
- 14.7. Informar imediatamente a SEFAZ as alterações de dados, como, por exemplo, endereços, telefones, nome de representantes, que possam influenciar a comunicação do CONTRATANTE com a CONTRATADA.
- 14.8. São expressamente vedadas à CONTRATADA:
- a) Veiculação de publicidade acerca do contrato, salvo se houver prévia autorização da CONTRATANTE.
 - b) Subcontratar ou transferir, no todo ou em parte, o objeto deste contrato.

15. DO MODELO DE GESTÃO DO CONTRATO

15.1. Modelo de Gestão do Contrato

- 15.1.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133/2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.
- 15.1.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o prazo de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.
- 15.1.3. As comunicações entre CONTRATANTE e CONTRATADA devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.
- 15.1.4. A CONTRATANTE poderá convocar representante da CONTRATADA para adoção de providências que devam ser cumpridas de imediato.

15.2. Fiscal do Contrato

- 15.2.1. São atribuições do fiscal de contratos, sem prejuízo das demais previstas no Manual de Gestão e Fiscalização dos Contratos Administrativos:

- a) Conhecer suas atribuições e responsabilidades para o exercício das atividades de fiscalização;
- b) Atestar, em documento hábil, a prestação do serviço após conferência prévia do objeto contratado;
- c) No caso de serviços, controlar a efetividade e eficácia da sua execução em estrita observância ao estabelecido no contrato (especificações e normas técnicas, por exemplo), solicitando a correção de eventuais vícios, imperfeições, deficiências e/ou omissões;
- d) Registrar todas as ocorrências havidas durante o período de execução do contrato, em livro próprio;
- e) Assegurar-se do cumprimento integral das obrigações contratuais assumidas pela contratada;
- f) Apresentar, periodicamente ou quando solicitado, relatório circunstanciado de acompanhamento da execução do serviço;
- g) Encaminhar as questões que ultrapassem suas atribuições ao Gestor do Contrato;
- h) Providenciar, sempre por escrito, a obtenção de esclarecimentos, auxílio ou suporte técnico para aqueles casos em que tiver dúvidas sobre a providência a ser adotada;
- i) Emitir atestados ou certidões de avaliação dos serviços prestados;
- j) Informar o Gestor do Contrato sobre irregularidade que deva ser sanada;
- k) Representar, levando ao conhecimento das autoridades a execução de ato ilícito que tenha tido conhecimento em razão de seu ofício.

15.3. **Gestor do Contrato**

15.3.1. São atribuições do Gestor de Contratos, sem prejuízo das demais previstas no Manual de Gestão e Fiscalização dos Contratos Administrativos:

- a) Gerenciar todo o Processo Administrativo de Despesa Pública – PADP referente à contratação;
- b) Assegurar-se do cumprimento integral das obrigações contratuais assumidas, com qualidade e em respeito à legislação vigente;
- c) Solicitar periodicamente ao fiscal do contrato relatório das ocorrências para que, sendo o caso, possa tomar as providências cabíveis a fim de corrigi-las;
- d) Analisar notas/glosas escritas pelo fiscal, a fim de constatar a possível necessidade de descontos a serem realizados no valor mensal dos serviços/compras, informando-as ao setor financeiro;
- e) Encaminhar formalmente as demandas ao preposto por meio de ordem de serviço/entrega ou fornecimento;
- f) Repassar ao Fiscal de Contratos todas as informações e documentos relativos ao contrato, para que este último possa bem fiscalizá-lo;
- g) Acompanhar a vigência do instrumento contratual, a fim de proceder às diligências administrativas de prorrogação, se possível e vantajoso for, ou ao encerramento da contratação, de modo a garantir o atendimento do interesse público.
- h) Propor medidas que melhorem a execução do contrato.
- i) Providenciar, sempre por escrito, a obtenção de esclarecimentos, auxílio ou suporte técnico, para aqueles casos em que tiver dúvidas sobre a providência a ser adotada.
- j) Negociar condições previamente estabelecidas com o contratante sempre que o mercado assim o exigir e quando da sua prorrogação, nos termos da Lei;
- k) Informar periodicamente ao Ordenador de Despesas do órgão/entidade sobre ocorrências relacionadas ao contrato;
- l) Notificar a contratada, por ordem do Ordenador de Despesas do órgão contratante, sobre irregularidades encontradas; e
- m) Controlar a regularidade do adimplemento das obrigações trabalhistas e previdenciárias da contratada com seus empregados;

16. **CRITÉRIOS DE PAGAMENTO E PREÇO**

16.1. Do Pagamento

16.2. O pagamento pelos serviços efetivamente prestados dar-se-á em parcelas e será creditado mensalmente à empresa CONTRATADA, ocorrendo no prazo não superior a 5 (cinco) dias úteis, contados do recebimento e atesto do documento fiscal/fatura - que deverá conter o endereço, o CNPJ, os números do Banco, da Agência e da Conta Corrente da Empresa contratada, o número da Nota de Empenho e a descrição clara do objeto - em moeda corrente nacional, de acordo com as condições constantes na proposta da Empresa contratada e aceita pela Administração contratante.

16.3. A emissão da ordem bancária será efetivada após o documento fiscal ser conferido, aceito e atestado por servidor responsável, caracterizando o recebimento definitivo, e ter sido verificada a regularidade da Empresa contratada, mediante consulta on-line ao Sistema Unificado de Cadastro de Fornecedores (SICAF), ao Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS), ao Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa disponível no Portal do CNJ e à Certidão Negativa (ou Positiva com efeito de Negativa) de Débitos Trabalhistas (CNDT), para comprovação, dentre outras coisas, do devido recolhimento das contribuições sociais (FGTS e Previdência Social) e demais tributos estaduais, federais e municipais, conforme cada caso.

16.4. O documento fiscal deverá ser emitido em nome da Secretaria de Estado da Fazenda (SEFAZ) - CNPJ nº 04.034.484/0001-40.

16.5. A empresa contratada deve apresentar o documento fiscal de fornecimento dos serviços, emitido e entregue ao fiscal do contrato, para fins de liquidação e pagamento.

16.6. Na ocorrência de rejeição do documento fiscal motivado por erro ou incorreções, ele será devolvido à empresa contratada para retificação e reapresentação, acrescendo-se, no prazo fixado para pagamento, os dias que se passarem entre a data da devolução e a da reapresentação.

16.7. Nos casos de eventuais atrasos injustificados de pagamento, desde que a Empresa contratada não tenha concorrido de alguma forma para tanto, fica convencionado que a taxa de compensação financeira devida pela Administração contratante, desde a data limite fixada para pagamento até a data do efetivo pagamento, será a seguinte: $EM = N \times VP \times I / 365$, onde: EM = Encargos moratórios a serem pagos pelo atraso de pagamento; N = Número de dias de atraso contados entre a data limite prevista para o pagamento e a data do efetivo pagamento; VP = Valor da parcela em atraso; e I = IPCA anual acumulado (Índice de Preços ao Consumidor Ampliado do IBGE) / 100.

16.8. Os documentos de cobrança deverão ser entregues pela empresa contratada, na SEFAZ, no horário de expediente da CONTRATANTE, ou por e-mail a ser informado quando da assinatura do contrato.

16.9. Em nenhuma hipótese será efetuado pagamento de documento fiscal com o número do CNPJ/MF diferente do que foi apresentado na proposta de preços, mesmo que sejam empresas consideradas matriz e filial ou vice-versa, ou pertencentes ao mesmo grupo ou conglomerado.

16.10. Não será realizado qualquer tipo de pagamento através de boleto bancário ou por outro meio diferente do previsto no Contrato.

16.11. A Administração CONTRATANTE, no momento do pagamento, providenciará as devidas retenções tributárias, nos termos da legislação vigente, exceto nos casos em que a empresa contratada comprovar, na forma prevista em lei, não lhe serem aplicáveis tais retenções.

16.12. Caso a empresa contratada seja optante pelo Sistema Integrado de Pagamento de Impostos e Contribuições das ME e EPP – SIMPLES, desde que não haja vedação legal para tal opção em razão do objeto executado, deverá apresentar, juntamente com o documento fiscal, a devida comprovação, a fim de evitar a retenção na fonte dos tributos e contribuições, conforme legislação em vigor.

16.13. Do Reajuste e Revisão

16.13.1. Os preços relativos aos serviços contratados serão fixos e irrevogáveis, durante o período de 12 (doze) meses, contado da data de assinatura do Contrato ou do último reajuste.

16.13.2. Após esse período, os preços poderão ser reajustados, mediante a aplicação de índice, de acordo com os Lotes, sendo:

I - Lotes I e II: **Índice IST** (Índice de Serviços de Telecomunicações), normatizado pela ANATEL através da Resolução nº 532, de 3 de agosto de 2009, ocorrido no período, ou por outro Índice que o venha a substituí-lo.

II - Lote III: **Índice ICTI** (Índice de Custo da Tecnologia da Informação), calculado pelo Instituto de Pesquisas Econômicas Aplicadas – IPEA, ocorrido no período, ou por outro Índice que o venha a substituí-lo.

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

16.14. Equilíbrio Econômico-Financeiro

16.14.1. Com vistas à manutenção do equilíbrio econômico financeiro do Contrato, poderá ser promovida revisão contratual, desde que eventuais solicitações nesse sentido estejam acompanhadas de comprovação da superveniência de fatos imprevisíveis ou previsíveis, porém de consequências incalculáveis, retardadores ou impeditivos da execução do ajustado, configurando álea econômica extraordinária e extracontratual, bem como de demonstração analítica de seu impacto nos custos do Contrato, nos termos da Lei nº 14.133/21.

17. DA FORMA DE SELEÇÃO DO FORNECEDOR**17.1. Modalidade**

17.1.1. Procedimento de licitação, na modalidade **PREGÃO**, sob a forma **ELETRÔNICA**, para **REGISTRO DE PREÇOS**, nos termos da **Lei 14.133/21**, especialmente art. 17, §2º, arts. 28 e 29.

17.1.2. Critério de Julgamento

17.1.3. Menor preço por lote.

17.2. Qualificação Técnica

17.2.1. As licitantes deverão comprovar que fornecem ou já forneceram satisfatoriamente os serviços em características e prazos compatíveis com todos os itens de cada lote que estarão concorrendo, mediante a apresentação de ATESTADO DE CAPACIDADE TÉCNICA fornecido por pessoa jurídica de direito público ou privado, em nome da Licitante, comprovando a execução de serviços iguais ou semelhantes dos quantitativos estabelecidos neste edital.

17.2.2. O atestado de capacidade técnica poderá ser apresentado em nome da matriz ou da filial do fornecedor.

17.2.3. A proponente deverá apresentar Declaração de que tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação.

17.2.4. A proponente deverá apresentar a DECLARAÇÃO DE VISTORIA (ANEXO II) ou a DECLARAÇÃO DE RENÚNCIA À VISTORIA TÉCNICA(ANEXO III). A não apresentação da DECLARAÇÃO será motivo de inabilitação.

17.2.4.1. A declaração poderá ser substituída por declaração formal assinada pelo responsável técnico do licitante acerca do conhecimento pleno das condições e peculiaridades da contratação.

17.2.5. Todos os documentos apresentados poderão ser alvo de diligência por parte da CONTRATANTE, podendo ser exigido, que apresente cópia autenticada do contrato ou da(s) respectiva(s) nota(s) fiscal(is), que deram origem ao atestado, sendo desclassificado o licitante que apresentar documentação falsa ou incompleta, estando sujeito, ainda, às penalidades previstas em lei.

17.2.6. Outras comprovações para os Lotes I e II:

a) A PROPONENTE deverá comprovar por meio de Atestado de Capacidade Técnica, fornecido por pessoa jurídica de direito público ou privado, declarando ter a empresa licitante fornecido ou estarem fornecendo serviço de limpeza contra ataques DDOS (Distributed Denial of Service);

b) Para fins de fornecimento dos links de acesso à Internet, a PROPONENTE deverá comprovar ser um provedor de backbone, devendo este ser um AS (Autonomous System) do protocolo BGP (Border Gateway Protocol) registrado.

c) A PROPONENTE deverá comprovar que possuem backbone IP próprio com saída com destino direto para no mínimo outros 2 (dois) backbones distintos do Brasil (AS's distintos), cada qual com capacidade de, no mínimo, **25 (vinte e cinco) Gbps**. Essas saídas deverão ser compostas por uma ou mais conexões entre o AS da Contratada e os AS's remotos;

d) A PROPONENTE deve comprovar estar ligada a no mínimo 02 PTT's (Ponto de Troca de Tráfego Nacionais);

e) A PROPONENTE deve comprovar ter conexão direta com um AS internacional com velocidade mínima de 10 Gbps;

f) A PROPONENTE deve apresentar atestado ou Declaração emitida pelo Fabricante da Solução de Anti-DDoS que a mesma suporta no mínimo 25 Gbps de limpeza de tráfego, implantada em seu backbone.

g) A PROPONENTE deverá comprovar através de atestados e registros de POPs na ANATEL que possui operação na Cidade de Rio Branco, sendo que este registro deverá constar a Razão Social e

o CNPJ da LICITANTE;

h) A PROPONENTE deverá apresentar Termo de autorização expedida pela ANATEL para prestação de Serviço de comunicação multimídia (SCM);

17.2.7. Outras comprovações para o **Lote III**:

a) Para fins de fornecimento da Solução de segurança de perímetro, a PROPONENTE deverá comprovar que é parceiro autorizado do fabricante da solução ofertada.

17.3. **Qualificação Econômico-Financeira**

17.3.1. O Patrimônio Líquido a ser exigido deve ser de 10% (dez por cento) do valor estimado da contratação.

17.4. **Prazo de Validade da Proposta**

17.4.1. O prazo de validade da proposta deverá ser, no mínimo, de 60 (sessenta) dias corridos, a contar da data de sua apresentação.

17.4.1.1. Na ausência de indicação expressa do prazo de validade, considerar-se-á tacitamente indicado o prazo de 60 dias.

17.4.2. Decorrido o prazo de validade das propostas, sem convocação para assinatura do Contrato, ficam os proponentes liberados dos compromissos assumidos.

18. ÓRGÃO GERENCIADOR DA ATA DE REGISTRO DE PREÇOS

18.1. A Secretaria de Estado da Fazenda do Acre (SEFAZ/AC) atuará como órgão gerenciador da Ata de Registro de Preços.

19. JUSTIFICATIVA PARA ESCOLHA DO SISTEMA DE REGISTRO DE PREÇOS - SRP

19.1. A escolha do Sistema de Registro de Preços (SRP), conforme disposto nos arts. 82 da Lei nº 14.133/2021, justifica-se plenamente diante da natureza e complexidade do objeto, que envolve serviços continuados de links de acesso à internet dedicados, proteção contra ataques DDoS e solução de proteção de perímetro gerenciado, com alta disponibilidade de hardware (cluster).

19.2. Trata-se de serviços estratégicos e de demanda permanente, cuja execução requer continuidade operacional, alta confiabilidade e flexibilidade para adequação às necessidades da Secretaria de Estado da Fazenda do Acre (SEFAZ/AC). O SRP permite a contratação conforme a necessidade e disponibilidade orçamentária ao longo do exercício, viabilizando maior eficiência administrativa e econômica, ao possibilitar a formação prévia de um cadastro de fornecedores qualificados, assegurando celeridade nas contratações subsequentes, sem comprometer os padrões de desempenho, segurança e conformidade técnica exigidos pela instituição.

19.3. Ademais, o uso do SRP é particularmente adequado diante da variabilidade na demanda de conectividade e segurança de rede, que pode oscilar conforme o volume de acessos aos sistemas corporativos, o crescimento da infraestrutura tecnológica e a necessidade de reforço da proteção contra ameaças cibernéticas. Essa sistemática permite que a SEFAZ/AC realize contratações rápidas e planejadas, com base em preços previamente registrados e validados, garantindo padronização técnica, competitividade, economicidade e transparência, princípios previstos no art. 5º da Lei nº 14.133/2021.

19.4. A adoção do Sistema de Registro de Preços também contribui para o planejamento e a continuidade dos serviços críticos de telecomunicações e segurança de dados, evitando interrupções que possam comprometer a operação fiscal e arrecadatória do Estado. Além de reduzir custos administrativos com repetidas licitações, o SRP assegura previsibilidade e agilidade na contratação de soluções tecnológicas atualizadas, ajustando-se à dinâmica da infraestrutura digital do órgão.

19.5. Portanto, o procedimento licitatório na modalidade Pregão Eletrônico, para Registro de Preços, encontra-se em plena conformidade com a Lei nº 14.133/2021 e o Decreto Estadual nº 11.363/2023, atendendo aos princípios da eficiência, economicidade, transparência, planejamento e continuidade. Tal escolha demonstra-se tecnicamente consistente e estratégica, assegurando a modernização da infraestrutura digital, a proteção dos sistemas institucionais e a continuidade dos serviços essenciais à missão da SEFAZ/AC.

20. DA PARTICIPAÇÃO DE CONSÓRCIOS

20.1. Participação de Consórcios

20.1.1. Não será admitido a participação de consórcios.

20.1.2. A vedação à participação de consórcios no presente procedimento licitatório atende ao interesse público ao prestigiar os princípios da competitividade, da economicidade e da eficiência. Não há elementos que justifiquem a admissão de empresas em consórcio, uma vez que o objeto licitado, embora estratégico, não se caracteriza como de grande vulto econômico nem apresenta peculiaridades que demandem a união de diferentes fornecedores para sua execução. Pelo contrário, trata-se de serviços que exigem alta disponibilidade, respostas rápidas a incidentes, confidencialidade no tratamento de dados e governança rigorosa, requisitos incompatíveis com a dispersão de responsabilidades típica dos consórcios. A fragmentação contratual fragilizaria a segurança, dificultaria a responsabilização por falhas e comprometeria a continuidade operacional.

20.1.3. A jurisprudência do Tribunal de Contas da União reforça essa diretriz ao reconhecer que, em serviços de elevada criticidade e complexidade, a responsabilização exclusiva do contratado é indispensável para assegurar a efetividade, a integridade e a segurança das soluções implementadas. Dessa forma, a vedação à participação de consórcios não constitui restrição indevida à competitividade, mas sim medida técnica e juridicamente necessária para garantir a execução plena e segura do contrato, resguardando as infraestruturas críticas e o interesse público.

21. ATA DE REGISTRO DE PREÇOS

21.1. Assinatura

21.1.1. Homologado o resultado da licitação, o licitante mais bem classificado terá o **prazo de 05 (cinco) dias**, contados a partir da data de sua convocação, para assinar a Ata de Registro de Preços, sob pena de decadência do direito à contratação, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021.

21.1.2. O prazo de convocação poderá ser prorrogado 1 (uma) vez, por igual período, mediante solicitação do licitante mais bem classificado ou do fornecedor convocado, desde que:

- I - a solicitação seja devidamente justificada e apresentada dentro do prazo; e
- II - a justificativa apresentada seja aceita pela Administração.

21.1.3. A Ata de Registro de Preços será assinada por meio de assinatura digital e disponibilizada no sistema de registro de preços.

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

21.2. Vigência

21.2.1. O prazo de vigência da ata de registro de preços será de 1 (um) ano, contado a partir do primeiro dia útil subsequente à data de divulgação no PNCP, podendo ser prorrogado por igual período, desde que comprovado o preço vantajoso, nos termos do art. 22, do Decreto nº 11.462, de 31 de março de 2023.

21.3. Alteração ou atualização dos preços registrados

21.3.1. Com vistas à manutenção do equilíbrio econômico-financeiro da ATA, poderá ser promovida revisão dos preços registrados, desde que eventuais solicitações estejam acompanhadas de comprovação da superveniência de fatos imprevisíveis ou previsíveis, porém de consequências incalculáveis, retardadores ou impeditivos da execução do ajustado, nos termos do disposto no art. 25, do Decreto nº 11.462/2023.

21.3.2. Da Adesão e Obrigações do Órgão Gerenciador/Detentor da Ata

21.3.3. Durante a vigência da ata, os órgãos e as entidades da Administração Pública federal, estadual, distrital e municipal que não participaram do procedimento de IRP poderão aderir à ata de registro de preços na condição de não participantes, observados os seguintes requisitos:

- a) apresentação de justificativa da vantagem da adesão, inclusive em situações de provável desabastecimento ou descontinuidade de serviço público;
- b) demonstração de que os valores registrados estão compatíveis com os valores praticados pelo mercado na forma do art. 23 da Lei nº 14.133, de 2021; e
- c) consulta e aceitação prévias do órgão ou da entidade gerenciadora e do fornecedor.

21.3.4. A autorização do órgão ou entidade gerenciadora apenas será realizada após a aceitação da adesão pelo fornecedor.

21.3.5. O órgão ou entidade gerenciadora poderá rejeitar adesões caso elas possam acarretar prejuízo à execução de seus próprios contratos ou à sua capacidade de gerenciamento.

21.3.6. Após a autorização do órgão ou da entidade gerenciadora, o órgão ou entidade não participante deverá efetivar a aquisição ou a contratação solicitada em até noventa dias, observado o prazo de vigência da ata.

21.3.7. O prazo de que trata o subitem anterior, relativo à efetivação da contratação, poderá ser prorrogado excepcionalmente, mediante solicitação do órgão ou da entidade não participante aceita pelo órgão ou pela entidade gerenciadora, desde que respeitado o limite temporal de vigência da ata de registro de preços.

22. DA ADEQUAÇÃO ORÇAMENTÁRIA

22.1. As despesas decorrentes da contratação correrão à conta dos recursos consignados abaixo, de acordo com a informação de Dotação Orçamentária:

22.2. Descrição da Dotação Orçamentária:

	CÓDIGO	DESCRIÇÃO
Órgão	715	Secretaria de Estado da Fazenda - SEFAZ
Unidade Orçamentária	001	Unidade Gestora
Programa de Trabalho	04.129.1466.1198.00.00	Modernização dos Sistemas de Arrecadação, Administração Financeira, Tributária e Contábil
Elemento de Despesa	33904000	Serviços de tecnologia da informação
Fonte de Recurso	100	Recursos Próprios do Tesouro

23. ANEXOS

23.1. Anexo I - Modelo de Termo de Confidencialidade

TERMO DE CONFIDENCIALIDADE

Pelo presente Termo de Confidencialidade, eu _____, CPF nº _____, RG nº _____, expedida pelo (a) _____, representante da empresa _____, CNPJ nº _____, declaro ter recebido da Secretaria de Estado da Fazenda do Acre - SEFAZ/AC informações confidenciais e reservadas do ambiente tecnológico, incluindo dados quantitativos e qualitativos da estrutura e topologia da rede, de sistemas, de métodos e processos atualmente utilizados, entre outras informações, todas obtidas com a intenção de fundamentar a proposta comercial, que se expostas ao domínio público permitem a ação deletéria de softwares maliciosos e hacker's, razão pelo qual, por meio do presente termo de confidencialidade a empresa signatária, participante da licitação em epígrafe, compromete-se a manter sob sigilo as informações e dados obtidos, e a eliminar todas as informações obtidas caso não seja sagrada vencedora do certame, sob as penas da Lei, comprometo-me a não divulgar as informações a que tive acesso.

Para os fins deste Termo, "informação confidencial" significa todos os esclarecimentos técnicos, minutas de documentos, documentos, dados, estudos, especificações técnicas, inovações ou aperfeiçoamento de que venham a ter acesso, ou que venham a lhes ser confiado em razão deste Termo, incluindo-se previsões, gráficos e todas e quaisquer outras informações, escritas, orais ou visuais, relacionadas com a apuração necessária ao conhecimento do ambiente de TIC e a formulação da proposta comercial da licitante, acerca do objeto da licitação, seja de natureza técnica, operacional, financeira, comercial e/ou legal, que possua valor tangível ou intangível para ao órgão CONTRATANTE, incluindo, mas não se limitando, a existência deste Termo e suas condições, mas excluindo: a) informações que estejam ou venham a estar em domínio do público em geral por outra forma que não seja a violação deste Termo; ou b) informações que a licitante pode comprovar que não foi adquirida, direta ou indiretamente, em caráter confidencial, neste ato; ou c) informações de propriedade dos órgãos, por eles divulgada, de maneira irrestrita e não confidencial; ou d) informações que tenham sua divulgação exigida por lei, incluindo por qualquer tribunal ou órgão regulatório com competência para tanto

Rio Branco - AC, [Data].

[Nome e cargo do representante da Contratada]
Empresa/CNPJ

23.2. **Anexo II - Modelo de Declaração de Vistoria Técnica**

DECLARAÇÃO DE VISTORIA TÉCNICA

Declaro, em atendimento ao previsto no Edital xx/xxxx e seus anexos do PREGÃO ELETRÔNICO SRP Nº XX/XXXX, que eu, _____, portador(a) da CI/RG nº _____ e do CPF nº _____, representante da empresa _____, estabelecida no(a) _____, como seu representante legal, para os fins da presente declaração, compareci perante o representante da SEFAZ/AC em Rio Branco/AC e vistoriei o ambiente computacional do mesmo, assim como inteirei-me sobre as condições e grau de dificuldades existentes envolvendo o parque tecnológico da CONTRATANTE e os serviços a serem executados com apoio dos profissionais, tomando plena ciência das condições e grau de dificuldade existentes e das condições para prestação dos serviços, estando satisfeita com as informações e esclarecimentos obtidos durante a visita, estando plenamente capaz de elaborar proposta para a licitação em tela, de modo a não incorrer em omissões que jamais poderão ser alegadas em favor de eventuais pretensões de inclusão de serviços ou acréscimos de preços.

Rio Branco - AC, [Data].

[Nome e cargo do representante da Contratada]

Visto:
Representante da SEFAZ-AC

23.3. **Anexo III - Modelo de Declaração de Renúncia da Vistoria Técnica**

DECLARAÇÃO DE RENÚNCIA DA VISTORIA TÉCNICA

Declaro, em atendimento ao previsto no Edital xx/xxxx e seus anexos do PREGÃO ELETRÔNICO SRP Nº XX/XXXX, que eu, _____, portador(a) da CI/RG nº _____ e do CPF nº _____, representante da empresa _____, estabelecida no(a) _____, como seu representante legal, para os fins da presente declaração, optamos pela não realização de vistoria técnica assumindo inteiramente a responsabilidade ou consequências por essa omissão, mantendo as garantias que vincularem nossa proposta

ao presente processo licitatório, em nome da empresa que represento, estando plenamente capaz de elaborar proposta para a licitação em tela, de modo a não incorrer em omissões que jamais poderão ser alegadas em favor de eventuais pretensões de inclusão de serviços ou acréscimos de preços.

Rio Branco - AC, [Data].

[Nome e cargo do representante da Contratada]

Visto:
Representante da SEFAZ-AC

23.4. Anexo IV - Modelo de Termo de Compromisso e Manutenção do Sigilo

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

INTRODUÇÃO

O Termo de Compromisso de Manutenção de Sigilo registra o comprometimento formal da Contratada em cumprir as condições estabelecidas no documento relativas ao acesso e utilização de informações sigilosas da Contratante em decorrência de relação contratual, vigente ou não.

Pelo presente instrumento a Secretaria de Estado da Fazenda do Acre (SEFAZ/AC), inscrita no CNPJ sob o n.º 04.034.484/0001-40, com sede temporária à Rua Vinte e Quatro de Janeiro, nº 35, Bairro Seis de Agosto - Rio Branco/AC, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.º <nº do contrato> doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE; CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção; CONSIDERANDO o disposto na Política de Segurança da Informação e Privacidade da CONTRATANTE;

Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições abaixo discriminadas.

1 – OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas disponibilizadas pela CONTRATANTE e a observância às normas de segurança da informação e privacidade por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei nº 13.709, de 14 de agosto de 2018 e demais normativos que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo na Administração Pública.

2 – CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquela abrangida pelas demais hipóteses legais de sigilo.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

3 – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

4 – DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

- I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;
- II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;
- III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

5 – DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento prévio e expresso da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmos judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de

atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

6 – VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

7 – PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 87 da Lei nº. 8.666/93.

8 – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, termos e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações, conforme definição do item 3 deste documento, disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

9 – FORO

A CONTRATANTE elege o foro da _____, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

10 – ASSINATURAS

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

[Contratada]

[Contratante]

[Testemunhas1] / [Testemunhas2]

23.5. Anexo V - Modelo de Termo de Ciência

TERMO DE CIÊNCIA

1 - INTRODUÇÃO

O Termo de Ciência visa obter o comprometimento formal dos empregados da contratada diretamente envolvidos na contratação quanto ao conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes no Órgão/Entidade.

No caso de substituição ou inclusão de empregados da contratada, o preposto deverá entregar ao Fiscal do Contrato os Termos de Ciência assinados pelos novos empregados envolvidos na execução dos serviços contratados.

2 - IDENTIFICAÇÃO

CONTRATO Nº	
OBJETO	
CONTRATADA/CNPJ	
PREPOSTO	
GESTOR DO CONTRATO (Matrícula)	

3 - CIÊNCIA

Por este instrumento, os funcionários abaixo identificados declaram ter ciência e conhecer o inteiro teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes da Contratante.

4 - FUNCIONÁRIOS DA CONTRATADA

NOME	MATRÍCULA	ASSINATURA

Rio Branco - AC, [Data].

24. RESPONSABILIDADES

Elaborado por:

DIVISÃO DE PROJETOS - DIPROJ

Requisitante/Revisor

ISRAEL JORDÃO SANTOS DE MELO

Chefe do Departamento de Tecnologia da Informação

Portaria nº 13/2023

*Vistos os autos, no uso de minhas atribuições, em cumprimento ao disposto no artigo 72, inciso VIII da Lei de Licitações e Contratos nº 14.133/2021, **AUTORIZO** a Licitação, ratificando a importância do objeto para o desempenho das atividades desta Unidade Administrativa e os elementos técnicos apresentados para fundamentar a contratação.*

Encaminha-se à Diretoria de Administração e Finanças para as demais providências.

José Amarísio Freitas de Souza
Secretário de Estado da Fazenda
Decreto nº 4.059-P/2023



Documento assinado eletronicamente por **ISRAEL JORDAO SANTOS DE MELO, Chefe(a) de Departamento**, em 27/11/2025, às 12:30, conforme horário oficial do Acre, com fundamento no art. 11, § 3º, da [Instrução Normativa Conjunta SGA/CGE nº 001, de 22 de fevereiro de 2018](#).



Documento assinado eletronicamente por **JOSE AMARÍSIO FREITAS DE SOUZA, Secretário(a) de Estado**, em 28/11/2025, às 09:50, conforme horário oficial do Acre, com fundamento no art. 11, § 3º, da [Instrução Normativa Conjunta SGA/CGE nº 001, de 22 de fevereiro de 2018](#).



A autenticidade deste documento pode ser conferida no site <http://www.sei.ac.gov.br/autenticidade>, informando o código verificador **0018430232** e o código CRC **12BF0519**.