TRIBUNAL DE CONTAS DO ESTADO DO AMAZONAS

Av. Efigênio Sales, 1155, - Bairro Parque 10, Manaus/AM, CEP 69055-736

TERMO DE REFERÊNCIA Nº 74/2026/SEGER/GP

PROCESSO nº 005280/2026

TRIBUNAL DE CONTAS DO ESTADO DO AMAZONAS
ENDEREÇO: AV. EFIGÊNIO SALLES, 1155 – PARQUE 10 DE NOVEMBRO – CEP 69.055-736
CNPJ: 05.829.742/0001-48

1. INTRODUÇÃO

1.1 Foi elaborado pela Secretaria Geral de Administração - SEGER e apoio técnico da Secretaria de Tecnologia da Informação - SETIN do Tribunal de Contas do Estado do Amazonas – TCE/AM o presente Termo de Referência, que servirá de base ao procedimento de contratação, fundamentado na Lei nº 14.133/2021 e nas normas aplicáveis ao Tribunal.

1.2 O procedimento será realizado por **licitação na modalidade Pregão Eletrônico, pelo Sistema de Registro de Preços – SRP**, com **critério de julgamento de menor preço global por lote único**, para formação de Ata de Registro de Preços destinada a futuras e eventuais contratações da solução integrada de segurança cibernética descrita neste Termo.

1.3 A modalidade, o julgamento e o registro de preços fundamentam-se nos arts. 6º, incisos XIII e XXIII, 18, 28, inciso I, 29, 33, inciso I, 40, 78, inciso IV, e 82 a 86 da Lei nº 14.133/2021, observadas as normas de regulamentação aplicáveis ao TCE/AM.

1.4 O quantitativo máximo a registrar é de **04 (quatro) equipamentos**, com suas respectivas subscrições, garantia e suporte, até 02 (dois) serviços de implantação de par em alta disponibilidade e 08 (oito) unidades de atualização de conhecimentos. A contratação inicial prevista compreende 02 (dois) equipamentos, os componentes correspondentes, 01 (um) serviço de implantação e as 08 (oito) unidades de capacitação.

1.5 A Ata de Registro de Preços terá vigência de **01 (um) ano**, contado conforme o marco definido no edital e na ata, podendo ser prorrogada por igual período, mediante comprovação de preço vantajoso e observância das normas aplicáveis, nos termos do art. 84 da Lei nº 14.133/2021.

1.6 A vigência da ata corresponde ao período para formalização das contratações decorrentes. **Não se confunde com a cobertura de 60 (sessenta) meses das subscrições, garantia e suporte de cada solução efetivamente contratada**, nem com o parcelamento anual de seu pagamento. Os contratos terão vigência própria, conforme o art. 84, parágrafo único, e os arts. 105 e 106 da Lei nº 14.133/2021, observados os pressupostos legais da contratação plurianual.

1.7 A existência de preços registrados não obriga o Tribunal a contratar o quantitativo integral ou qualquer quantidade mínima, nos termos do art. 83 da Lei nº 14.133/2021. Cada contratação dependerá de necessidade administrativa, autorização competente e disponibilidade orçamentária.

1.8 O edital exigirá cotação integral dos quantitativos máximos do lote, não admitindo proposta para apenas parte dos itens ou em quantidade inferior à máxima prevista. Serão discriminados os preços unitários e totais de todos os componentes, assegurada a contratação inicial parcial nos quantitativos da tabela 4.1.

1.9 O TCE/AM atuará como órgão gerenciador. Na fase preparatória, observar-se-á o procedimento de intenção de registro de preços previsto no art. 86, admitida sua dispensa quando o Tribunal for o único contratante. A participação de outros órgãos, se admitida, exigirá prévia consolidação das demandas e dos quantitativos no edital.

1.10 A ata e o edital disciplinarão a convocação para assinatura, o cadastro de reserva e sua ordem de preferência, as condições para alteração dos preços registrados e as hipóteses de cancelamento, conforme o art. 82 e o regulamento aplicável. A unidade gerenciadora controlará os quantitativos contratados e os saldos de cada item.

1.11 Eventual adesão por órgão não participante dependerá de previsão no edital e na ata, das condições do regulamento aplicável, de justificativa de vantagem, comprovação da compatibilidade dos preços e aceitação prévia do gerenciador e do fornecedor, observados os limites do art. 86. Este registro contém quantitativos máximos expressamente definidos e não adota a hipótese de registro sem quantitativo total do art. 82, § 3º.

2. OBJETO E OBJETIVOS

BASE LEGAL: art. 6º, inciso XXIII, alínea “a”; art. 18; e art. 40 da Lei nº 14.133/2021.

2.1 O presente Termo tem como objeto a **formação de Ata de Registro de Preços para futura e eventual contratação de empresa especializada no fornecimento de até 04 (quatro) equipamentos de Firewall de Próxima Geração Palo Alto Networks PA-1420**, para composição de até 02 (dois) pares em alta disponibilidade, contemplando hardware com fontes redundantes, subscrições completas de segurança, GlobalProtect/Prisma Access Agent, garantia e suporte técnico por **60 (sessenta) meses**, instalação, configuração, migração e atualização de conhecimentos, conforme este Termo e o Estudo Técnico Preliminar – Tecnologia nº 10/2026/DIOTI/SETIN (0922764).

2.1.1 A aquisição inicial prevista corresponde a **02 (dois) equipamentos** para o ambiente principal do TCE/AM. Os outros 02 (dois) equipamentos destinam-se a eventual implantação ou evolução de site de contingência, condicionada ao desenvolvimento do projeto, à necessidade administrativa e à disponibilidade orçamentária.

2.2 **Objetivos específicos:**

a) garantir a continuidade da proteção perimetral e das demais camadas de segurança do ambiente tecnológico do TCE/AM;

b) preservar a disponibilidade, a integridade e a confidencialidade das informações institucionais;

c) atualizar tecnologicamente os firewalls atualmente utilizados pelo Tribunal;

d) assegurar a operação de **dois equipamentos em alta disponibilidade no ambiente principal e, se contratado, de um segundo par no site de contingência**, de modo que a indisponibilidade de um deles não interrompa a proteção e os serviços dependentes da solução;

e) manter o **GlobalProtect** para acesso remoto seguro aos sistemas internos por servidores em teletrabalho e demais usuários autorizados;

f) disponibilizar atualizações das bases de ameaças, funcionalidades de segurança, garantia e suporte especializado durante **60 meses**; e

g) promover a capacitação da equipe técnica responsável pela administração e pelo acompanhamento da solução.

3. JUSTIFICATIVA DA NECESSIDADE DA CONTRATAÇÃO

3.1 O TCE/AM dispõe de infraestrutura tecnológica corporativa que sustenta sistemas de fiscalização, processos eletrônicos, atividades administrativas e serviços prestados aos jurisdicionados e à sociedade. A proteção do tráfego que entra e sai dessa infraestrutura é essencial à continuidade das atividades institucionais e à segurança dos ativos de informação.

3.2 Entre as camadas de proteção utilizadas pelo Tribunal está o **Firewall de Próxima Geração – NGFW**, responsável por inspecionar e controlar o tráfego de dados entre a rede institucional e a Internet. A solução permite identificar aplicações e usuários, aplicar regras de segurança, prevenir ameaças e filtrar acessos a endereços e domínios conforme as políticas estabelecidas pela SETIN.

3.3 A infraestrutura está exposta a ameaças como vírus, phishing, códigos maliciosos, exploração de vulnerabilidades, tentativas de acesso indevido e exfiltração de dados. A operação de um firewall sem atualizações e subscrições vigentes reduz a capacidade de prevenção, detecção e resposta a esses eventos, elevando o risco de comprometimento das informações e de indisponibilidade dos sistemas.

3.4 O acesso remoto tornou-se parte das atividades do Tribunal. A subscrição **Prisma Access Agent/GlobalProtect** permite estabelecer conexão segura entre os dispositivos dos usuários autorizados e os sistemas internos, inclusive durante o teletrabalho. A interrupção dessa funcionalidade pode prejudicar as atividades desempenhadas fora das dependências físicas do TCE/AM.

3.5 Conforme registrado no ETP, o suporte técnico do fabricante e o direito de atualização das bases de ameaças das licenças atualmente utilizadas têm previsão de expiração em **07 de novembro de 2026**. A continuidade da solução após esse marco, sem as respectivas atualizações e coberturas, ampliaria a exposição da infraestrutura a incidentes de segurança.

3.6 O Tribunal utiliza atualmente equipamentos **Palo Alto PA-3220**. O ETP registra que a versão mais recente do sistema operacional compatível com esses equipamentos é o **PAN-OS 11.1**, cujo fim de suporte está previsto para **03 de maio de 2027**, segundo a documentação técnica indicada nos autos. A proximidade desse marco reforça a necessidade de atualização tecnológica, pois a permanência em plataforma sem suporte comprometeria o recebimento futuro de correções, inclusive para vulnerabilidades de segurança.

3.7 A contratação proposta prevê o registro de até **04 (quatro) equipamentos PA-1420**, com aquisição inicial de **02 (dois) equipamentos**. Esse quantitativo decorre da necessidade de formar um **par em alta disponibilidade**: caso um equipamento fique indisponível, o outro poderá manter a operação do ambiente e a aplicação das regras de segurança. Cada equipamento deverá contar com as respectivas subscrições, garantia, suporte e fonte adicional de alimentação para redundância.

3.8 A solução compreende funcionalidades de prevenção avançada de ameaças, filtragem de URL, análise de arquivos e proteção contra ameaças desconhecidas, segurança de DNS, recursos de SD-WAN e proteção de dispositivos. A contratação conjunta das funcionalidades é necessária para que o hardware opere com as camadas de proteção previstas no ETP durante todo o período de cobertura.

3.9 Além do fornecimento dos equipamentos e licenças, são necessários serviços especializados de instalação física, configuração, ativação, migração das regras e políticas atualmente utilizadas, testes e acompanhamento do funcionamento da nova solução. Esses serviços reduzem o risco de falhas na transição e permitem validar a operação do par em alta disponibilidade antes do recebimento definitivo.

3.10 A atualização de conhecimentos da equipe técnica integra a contratação para que os servidores responsáveis disponham de formação compatível com a administração, o diagnóstico e o acompanhamento da solução implantada. O ETP prevê treinamento oficial, material e ministração em português, além dos vouchers de treinamento e certificação nele especificados.

3.11 A cobertura de 60 (sessenta) meses foi examinada pela SETIN em comparação com alternativas de 36 meses. Desse modo, optou-se pela contratação das licenças/ subscrições com cobertura de 05 (cinco) anos e o desembolso em parcelas anuais, destacando a continuidade da proteção e do suporte e a previsibilidade orçamentária. A anualidade refere-se à forma de pagamento das licenças/ subscrições e não à redução da cobertura da solução para 12 (doze) meses.

3.12 A aquisição está alinhada ao **Objetivo Estratégico 3 do Planejamento Estratégico do TCE/AM 2025–2028**, relativo à modernização e otimização de processos com segurança da informação, tecnologia, capacitação e inovação. A demanda está prevista no **item 83 do Plano Anual de Contratação de 2026**.

3.13 A opção pelo SRP decorre da existência de demanda imediata definida para um par no ambiente principal e de demanda futura estimada, condicionada à implantação ou evolução do site de contingência. O registro permite contratar o par principal e preservar a possibilidade de aquisição posterior do segundo par durante a vigência da ata, sem antecipar a compra de equipamentos ainda sem utilização imediata.

3.14 A modelagem reduz o risco de aquisição desnecessária, preserva a padronização tecnológica e permite atender à evolução da infraestrutura sem novo certame para componentes de mesma natureza e especificação, caso a demanda futura se concretize. O quantitativo registrado constitui limite máximo estimado, e não obrigação de compra.

3.15 A indicação da marca e do modelo decorre da padronização e compatibilidade com a plataforma existente, em uso há mais de oito anos, e da necessidade de preservar integrações, políticas de segurança e conhecimentos da equipe técnica, conforme a justificativa do ETP e o art. 41, inciso I, alíneas “a” e “b”, da Lei nº 14.133/2021. A competição ocorrerá entre fornecedores aptos a entregar a solução, com comprovação do atendimento às especificações.

3.16 Diante da criticidade dos serviços protegidos, da necessidade de atualização tecnológica e da previsão condicionada de expansão, justifica-se a formação de Ata de Registro de Preços por **Pregão Eletrônico**, em lote único, para a solução integrada descrita neste Termo.

4. DESCRIÇÃO DETALHADA DA PROPOSTA

4.1 **Tabela de especificações e quantitativos – LOTE ÚNICO**

Nº	Produto ou serviço	Máximo na ata	Aquisição inicial

1	Appliance Palo Alto Networks PA-1420 (PAN-PA-1420-AC), incluindo fonte adicional AC de 450 W para redundância (PAN-PWR-450W-AC)	4	2
2	PA-1420 Core Security Subscription Bundle/Precision AI: Advanced Threat Prevention, Advanced URL Filtering, Advanced WildFire, Advanced DNS Security, Advanced SD-WAN e Device Security	4	2
3	GlobalProtect/Prisma Access Agent para appliances em alta disponibilidade (PAN-PA-1420-PAA-5YR-HA2)	4	2
4	Garantia e suporte Premium/Backline, em português por Centro de Suporte Autorizado, com retaguarda do fabricante e cobertura 24x7 (PAN-SVC-BKLN-1420-5YR)	4	2
5	Instalação, configuração, testes, repasses técnicos e migração da solução	2	1
6	Atualização de conhecimentos da tecnologia, com conteúdo, carga horária, participantes, vouchers e certificados especificados neste Termo	8	8

4.1.1 Os quantitativos dos itens 2, 3 e 4 acompanham os equipamentos efetivamente adquiridos. O item 5 corresponde à implantação de um par, inclusive o cabo de interligação. A demanda inicial contempla integralmente as 08 unidades do item 6, sem duplicação por aquisição posterior do segundo par. O licenciamento deverá ser suficiente para todos os appliances do par, conforme a métrica comercial do fabricante.

4.1.2 O fornecimento do item 1 compreende a fonte de alimentação adicional AC de **450 W** para cada PA-1420, destinada a completar a redundância de alimentação, conforme especificação do ETP.

4.1.3 Os serviços do item 5 abrangem, entre outras atividades previstas no ETP:

a) reunião prévia para definição dos requisitos, da arquitetura e da topologia da instalação;

b) instalação física dos equipamentos e interligação do par de alta disponibilidade, com fornecimento do cabo especificado no ETP;

c) energização e conexão dos equipamentos;

d) registro dos appliances junto ao fabricante e ativação das subscrições adquiridas;

e) atualização do PAN-OS e das bases de conteúdo contratadas;

f) configuração de interfaces, zonas, regras de segurança, NAT, objetos e perfis de segurança;

g) levantamento da arquitetura, das regras e das políticas da solução existente;

h) elaboração e execução de plano de migração aprovado pela SETIN; e

i) testes funcionais, transferência do tráfego e monitoramento do ambiente implantado.

4.1.4 As 08 (oito) unidades do item 6 destinam-se à capacitação de 08 (oito) participantes indicados pela SETIN. Os serviços deverão ser ministrados **em português**, por profissional certificado pelo fabricante, com material de apoio em português e **carga horária mínima de 40 horas**, abrangendo os treinamentos oficiais **Firewall Essentials (EDU-210)** e **Panorama: Managing Firewalls at Scale (EDU-220)**. Deverão ser fornecidos **02 vouchers** do treinamento **Firewall: Troubleshooting (EDU-330)** e **02 vouchers** para a prova de certificação **Palo Alto Networks Certified Next-Generation Firewall Engineer**, além dos certificados de participação, **conforme o ETP. Os vouchers previstos são quantitativos totais do item de capacitação, não multiplicados por participante.**

4.1.5 Integra este Termo o **Anexo I – Especificações técnicas e requisitos mínimos**, que deverá ser integralmente atendido pela solução fornecida.

4.2 **Valores estimados e orçamento sigiloso**

4.2.1 A estimativa de preços será instruída nos autos com a pesquisa e o mapa comparativo referentes ao **quantitativo máximo registrado e à cobertura de 60 (sessenta) meses**, consideradas as condições de pagamento anual e, separadamente, a aquisição inicial de 02 equipamentos, 01 implantação e 08 unidades de capacitação. A Administração deverá concluir a conferência dos cálculos das propostas antes de aprovar o orçamento estimado.

4.2.2 **O orçamento estimado terá caráter sigiloso na fase externa**, nos termos do **art. 24 da Lei nº 14.133/2021**, mediante a justificativa constante dos autos. O sigilo busca preservar a competitividade e estimular a apresentação dos melhores preços globais. Serão divulgados os quantitativos, as especificações e as demais informações necessárias à elaboração das propostas; o sigilo não prevalecerá para os órgãos de controle interno e externo.

4.2.3 A planilha estimativa, os preços referenciais por item, as memórias de cálculo e seus documentos de suporte deverão integrar os autos com o tratamento de acesso correspondente ao orçamento sigiloso.

4.3 A licitante deverá apresentar **declaração de atendimento integral** às especificações e condições deste Termo, discriminando preços unitários, totais por item, valor global do lote para o quantitativo máximo e a cobertura de 60 meses, bem como os desembolsos anuais das contratações efetivas. O preço unitário de cada item permitirá apurar o valor da aquisição inicial sem cobrar componentes não contratados.

4.4 **Justificativa do lote único e do não parcelamento**

4.4.1 O registro será adjudicado em **lote único**, conforme a análise de viabilidade técnica e econômica do ETP, os arts. 18, § 1º, inciso VIII, 40, inciso V, alínea “b”, e 82, § 1º, da Lei nº 14.133/2021. A aquisição em etapas dos pares não implica parcelamento da adjudicação entre fornecedores.

4.4.2 O parcelamento entre fornecedores distintos de hardware, subscrições, garantia, implantação e migração é inviável para esta solução integrada, pois pode produzir incompatibilidade entre equipamentos e licenças, lacunas de cobertura, conflito de responsabilidade técnica em incidentes críticos e dificuldades na correção de falhas durante a migração ou a operação. Neste ponto, a contratação parcelada poderia incorrer em apontamentos divergentes entre o fornecedor do equipamento e o fornecedor do serviço de suporte.

4.4.3 O lote único permite atribuir a uma contratada a responsabilidade pela entrega e pelo funcionamento da solução completa, sem afastar a necessidade de **discriminar os preços de todos os seus componentes** na proposta, na ata e em cada contrato.

4.4.4 A aceitabilidade abrangerá o valor global e os preços unitários máximos, definidos no orçamento estimado e tratados no edital em conformidade com seu sigilo. A contratação isolada de item do grupo, se necessária, dependerá de pesquisa prévia de mercado e demonstração de vantagem, conforme o art. 82, § 2º.

4.4.5 O registro dos preços e a aquisição parcial não dispensam o fornecimento de solução funcional completa para cada par contratado. Não serão cobrados equipamentos, subscrições ou serviços relativos ao segundo par antes de sua efetiva contratação.

4.4.6 A proposta de contratação em pares por esta Corte de Contas, do equipamento ou do serviço, não regulam ou impedem que a contratação dos itens possam, em algum momento, ser realizada de forma individual, seja do participamente da SRP ou do não participante, na forma de Adesão.

5. VISITA TÉCNICA

5.1 A empresa interessada poderá realizar, **mediante agendamento**, vistoria técnica **opcional** às instalações do TCE-AM, no período da publicação até **48 (quarenta e oito) horas úteis** antes da sessão.

5.2 A visita destina-se à verificação **in loco** das características do prédio, do **Data Center** e da infraestrutura relacionada, **sem** que a ausência de vistoria possa justificar alegações futuras de equívoco de dimensionamento.

5.3 A vistoria será realizada no **Data Center do TCE-AM**, na **Av. Efigênio Salles, 1155 – Parque 10 de Novembro - Manaus/AM**.

5.4 A licitante poderá realizar visita técnica para conhecimento do local, da infraestrutura e das condições de execução dos serviços, sendo facultada sua substituição por declaração formal do responsável técnico de pleno conhecimento dessas condições, não podendo posteriormente alegar desconhecimento para justificar prejuízos ou dificuldades na execução contratual, nos termos do art. 63, §§ 2º e 3º, da Lei nº 14.133/2021.

6. ENTREGA / PRAZO / RECEBIMENTO (arts. 6º, X; 40, §1º, II; 95 da Lei nº 14.133/2021)

6.1 **Vigência da ata:** 01 (um) ano, prorrogável por igual período nas condições do item 1.5. As contratações deverão ser formalizadas durante sua vigência e observar os saldos registrados.

6.2 **Vigência contratual e cobertura:** cada contrato deverá abranger o fornecimento, a implantação e **60 (sessenta) meses de subscrições, garantia e suporte**, contados do recebimento definitivo da solução implantada. A ativação técnica anterior necessária aos testes não poderá reduzir a fruição integral dessa cobertura. A vigência contratual deverá ser compatível com esses marcos e com os arts. 105 e 106 da Lei nº 14.133/2021.

6.3 **Entrega dos equipamentos:** o edital e o contrato fixarão prazo objetivo contado do recebimento da ordem de fornecimento, mediante consolidação técnica pela SETIN, considerando que as propostas juntadas aos autos indicam prazos entre **30 (trinta) e 90 (noventa) dias**. A necessidade de continuidade da proteção após 07/11/2026 deverá ser contemplada no planejamento da transição.

6.4 **Implantação e migração:** o cronograma do **Anexo II** prevê oito etapas e **124 horas técnicas**. A contratada apresentará à SETIN, antes de intervir no ambiente de produção, cronograma datado, responsáveis, dependências, janelas de mudança, testes, plano de reversão e data de conclusão, respeitando o prazo máximo de implantação consolidado no edital e no contrato. Horas técnicas representam esforço estimado, não prazo corrido de entrega.

6.5 A execução ocorrerá nas dependências do TCE/AM, à Av. Efigênio Salles, nº 1155, Manaus/AM, sob fiscalização da SETIN. Entregas deverão ser agendadas e realizadas até as 15h. Intervenções com impacto na disponibilidade dependerão de programação e autorização da fiscalização.

6.6 O recebimento observará o art. 140 da Lei nº 14.133/2021. O recebimento provisório será formalizado pela fiscalização após a entrega e a implantação, para verificação inicial. O recebimento definitivo será realizado após a conferência dos equipamentos e acessórios, ativação das subscrições e coberturas, conclusão da migração, documentação e aprovação dos testes funcionais, de segurança e de alta disponibilidade.

6.7 O treinamento terá recebimento próprio, condicionado à comprovação da participação, da carga horária, do material em português, dos certificados e da disponibilização dos vouchers. Nenhum componente não executado poderá ser incluído no atesto da parcela correspondente.

6.8 Eventual ampliação dos prazos deverá ser formalmente justificada, analisada pela fiscalização e autorizada pela Administração, observadas as hipóteses legais e as consequências contratuais. O recebimento não afasta a responsabilidade por vícios ou defeitos.

7. GARANTIA, SUPORTE TÉCNICO, CONDIÇÕES DE FORNECIMENTO E CERTIFICAÇÃO

7.1 As subscrições, a garantia e o suporte técnico de cada equipamento PA-1420 efetivamente contratado deverão permanecer ativos por **60 (sessenta) meses**, conforme as condições previstas no ETP, no edital e no contrato.

7.2 A CONTRATADA deverá efetuar **manutenção corretiva imediata** ao detectar mau funcionamento, restabelecendo o pleno funcionamento, observados os níveis de serviço contratados.

7.3 Nos chamados de atendimento, a CONTRATADA deverá fornecer à CONTRATANTE o **número do chamado técnico**, inclusive quando aberto junto ao **suporte do fabricante**.

7.4 O atendimento deverá estar disponível **24 horas por dia, 7 dias por semana**, em português. Os tempos máximos de resposta inicial, contados da abertura do chamado, serão:

Severidade	Situação	Resposta inicial
Crítica	Produto fora do ar, produção criticamente afetada e ausência de solução paliativa	Inferior a 1 hora
Alta	Produção em funcionamento, mas comprometida, sem solução paliativa	Até 2 horas
Média	Falha de funcionalidade sem impacto na produção, com solução paliativa	Até 4 horas
Baixa	Solicitações não críticas de informações, funcionalidades ou documentação	Até 8 horas

7.4.1 A reposição de hardware observará o plano Partner Enabled Premium/Backline, com previsão de próximo dia útil (NBD), sujeita à cobertura da localidade. A contratada deverá comprovar as condições de atendimento em Manaus e discriminar o prazo de entrega local antes da aprovação final da contratação. Prazo de resposta não equivale a prazo de solução definitiva.

7.4.2 A execução será apurada mensalmente mediante relatórios de chamados e monitoramento. O índice de cumprimento será a razão percentual entre chamados com resposta tempestiva e chamados válidos do mês; na ausência de chamados, não haverá desconto por esse indicador. Eventos de força maior ou decorrentes exclusivamente de ação ou omissão do TCE/AM, devidamente comprovados, serão excluídos.

7.4.3 Sobre o valor mensal de referência do item afetado, obtido pela divisão de sua parcela anual por 12, aplicar-se-á ajuste de 0% para cumprimento integral; 5% para índice de 90% a menos de 100%; 10% para índice de 80% a menos de 90%; e 20% para índice abaixo de 80%, com notificação e plano corretivo nesta última hipótese. Os ajustes não alteram a periodicidade anual de pagamento e serão deduzidos de valores devidos ou cobrados após a apuração, assegurada a manifestação da contratada.

7.4.4 A reincidência de índice inferior a 90% por três meses consecutivos ensejará apuração administrativa para eventual aplicação das sanções cabíveis. Ajustes remuneratórios serão distinguidos de multas administrativas, sem duplicação indevida de penalidade pelo mesmo fato.

7.5 A contratada deverá manter registros dos chamados, das providências adotadas e dos tempos de atendimento, disponibilizando-os à fiscalização para verificação da execução contratual.

8. CRITÉRIOS DE ACEITAÇÃO

8.1 O objeto será **aprovado pela SETIN**, em conformidade com este Termo, o ETP e a proposta vencedora.

8.2 Os equipamentos, licenças e serviços devem ser entregues em **perfeitas condições**; a CONTRATANTE poderá **recusar** entregas que não atendam ao **controle de qualidade** e às especificações técnicas.

8.3 Em caso de não conformidade dos equipamentos ou serviços, a entrega poderá ser **rejeitada no todo ou em parte**, aplicando-se as correções e penalidades previstas.

8.4 A aceitação definitiva da implantação exigirá a verificação da operação do par em alta disponibilidade, da aplicação das políticas de segurança, do funcionamento do GlobalProtect e da ativação das subscrições e coberturas contratadas.

9. QUALIFICAÇÃO TÉCNICA

9.1 **Atestado de Capacidade Técnica**, emitido por pessoa jurídica de direito público ou privado, compatível com o fornecimento ou a implantação de solução de firewall de características semelhantes às do objeto.

9.2 **Certificação técnica** da solução ofertada, emitida pelo **fabricante (Palo Alto Networks)**, conforme as condições e a comprovação exigidas no edital.

9.3 Deverá ser comprovada a capacidade de fornecer o suporte especificado e de executar os serviços de instalação, migração e atualização de conhecimentos previstos no ETP.

9.4 As exigências de habilitação técnica observarão o art. 67 da Lei nº 14.133/2021, limitando-se ao necessário para demonstrar capacidade de execução. A documentação técnica do produto e a certificação dos profissionais responsáveis deverão observar sua finalidade e o momento de apresentação previstos no edital.

10. OBRIGAÇÕES DA CONTRATADA (art. 92, XIV, XVI e XVII)

10.1 Entregar o serviço no local e prazos indicados neste TR.

10.2 Não transferir para outrem, no todo ou em parte, o contrato, sem anuência do TCE-AM.

10.3 Indicar **responsável técnico e contatos** para comunicação e notificações.

10.4 Responder por **todos os tributos e encargos** decorrentes da prestação.

10.5 **Reparar/corrigir/substituir**, às suas expensas, serviços com vícios/defeitos.

10.6 Responder por **perdas e danos** causados ao TCE-AM ou a terceiros.

10.7 Permitir o **acompanhamento/fiscalização** do TCE-AM.

10.8 Arcar com custos de **logística/devolução/acionamento de garantia** quando aplicável.

11. OBRIGAÇÕES DA CONTRATANTE (art. 92, X, XI e XIV)

11.1 Exigir o cumprimento integral do TR e anexos.

11.2 Receber o objeto nos prazos e condições previstas.

11.3 Notificar o contratado sobre **vícios/defeitos**, para correção.

11.4 **Acompanhar e fiscalizar** a execução contratual.

11.5 A Administração **não responde** por compromissos do contratado com terceiros.

11.6 Fiscalizar a **continuidade dos serviços**.

11.7 Efetuar o **pagamento** na forma e prazos deste instrumento.

11.8 Comunicar **irregularidades/atos ilícitos** aos órgãos competentes.

11.9 Emitir **relatórios** em todos os atos relativos à execução (sanções, alterações e repactuações).

12. INFRAÇÕES E SANÇÕES ADMINISTRATIVAS (PENALIDADES)

12.1 Constituem infrações administrativas (Lei nº 14.133/2021) as condutas elencadas nas alíneas **a** a **l** a seguir — incluindo **inexecução parcial/total**, **atrasos injustificados**, **documentação falsa**, **fraudes**, **comportamento inidôneo**, entre outras:

a) der causa à inexecução parcial do contrato;

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

c) der causa à inexecução total do contrato;

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

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

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

g) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

h) apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante o **Pregão Eletrônico** ou execução do contrato;

i) fraudar a contratação ou praticar ato fraudulento na execução do contrato;

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

k) praticar atos ilícitos com vistas a frustrar os objetivos da contratação;

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

12.2 Sanções aplicáveis:

i) **Advertência** (art. 156, §2º);

ii) **Impedimento de licitar e contratar** (art. 156, §4º);

iii) **Declaração de inidoneidade** (art. 156, §5º);

iv) **Multas**:

(1) **moratória** de **1% ao dia** sobre a parcela inadimplida, até **30 dias**;

(2) **compensatória** de **10%** sobre o **valor total** do contrato (inexecução total) ou sobre a **parcela inadimplida** (inexecução parcial).

12.3 A aplicação de sanções **não exclui** a obrigação de **reparação integral** do dano (art. 156, §9º).

12.4 As sanções poderão ser aplicadas **cumulativamente** com multa (art. 156, §7º).

12.4.1. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157).

12.4.2. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pela Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente (art. 156, §8º).

12.4.3. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

12.4.4 A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

12.5 Na aplicação das sanções serão considerados os critérios do art. 156, § 1º:

a) a natureza e a gravidade da infração cometida;

b) as peculiaridades do caso concreto;

c) as circunstâncias agravantes ou atenuantes;

d) os danos que dela provierem para a Contratante;

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

12.6. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159).

12.7. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160).

12.7.1 A Contratante deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal. (Art. 161)

12.7.2 As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21.

13. MODELO DE GESTÃO DO CONTRATO (art. 6º, XXIII, “f”, da Lei nº 14.133/2021)

13.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial (Lei nº 14.133/2021, art. 115, caput).

13.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila (Lei nº 14.133/2021, art. 115, §5º).

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

13.3.1. O fiscal do contrato anotará em registro próprio todas as ocorrências relacionadas à execução do contrato, determinando o que for necessário para a regularização das faltas ou dos defeitos observados (Lei nº 14.133/2021, art. 117, §1º).

13.3.2. O fiscal do contrato informará a seus superiores, em tempo hábil para a adoção das medidas convenientes, a situação que demandar decisão ou providência que ultrapasse sua competência (Lei nº 14.133/2021, art. 117, §2º).

13.4. O contratado será obrigado a reparar, corrigir, remover, reconstruir ou substituir, a suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes de sua execução ou de materiais nela empregados (Lei nº 14.133/2021, art. 119).

13.5. O contratado será responsável pelos danos causados diretamente à Administração ou a terceiros em razão da execução do contrato, e não excluirá nem reduzirá essa responsabilidade a fiscalização ou o acompanhamento pelo contratante (Lei nº 14.133/2021, art. 120).

13.6. Somente o contratado será responsável pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do contrato (Lei nº 14.133/2021, art. 121, caput).

13.7 A inadimplência do contratado em relação aos encargos trabalhistas, fiscais e comerciais não transferirá à Administração a responsabilidade pelo seu pagamento e não poderá onerar o objeto do contrato (Lei nº 14.133/2021, art. 121, §1º).

13.8. As comunicações entre o órgão e a contratada serão realizadas por escrito sempre que o ato exigir formalidade, admitido meio eletrônico que permita comprovar seu conteúdo e recebimento.

13.9. A Administração poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

13.10. Antes do pagamento da nota fiscal ou da fatura, deverá ser consultada a situação da empresa junto ao SICAF.

13.11. Serão exigidos a Certidão Negativa de Débito (CND) relativa a Créditos Tributários Federais e à Dívida Ativa da União, CND Relativa aos Débitos da Fazenda Estadual, Municipal, o Certificado de Regularidade do FGTS (CRF) e a Certidão Negativa de Débitos Trabalhistas (CNDT), caso esses documentos não estejam regularizados no SICAF.

14. PROCESSO DE PAGAMENTO (art. 92, V e VI, da Lei nº 14.133/2021)

14.1 PREÇO

14.1.1 O valor de cada contratação será calculado pelos preços unitários registrados e pelos quantitativos efetivamente contratados, com discriminação dos componentes de fornecimento único e da cobertura de **60 (sessenta) meses**. O pagamento será anual, em uma parcela por ano, sem cobrança de itens do saldo não contratado. O cronograma financeiro de cada contrato deverá evidenciar as cinco parcelas anuais e os marcos de execução que autorizam o pagamento.

14.1.2 No item acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

14.2 FORMA DE PAGAMENTO

14.2.1 O pagamento será realizado **anualmente, em parcela única por ano**, por ordem bancária para crédito em banco, agência e conta corrente indicados pela contratada, observados a execução e o atesto das obrigações correspondentes, a emissão de nota fiscal e a regular liquidação.

14.2.2 Será considerada data do pagamento o dia da emissão da ordem bancária.

14.2.3 **Primeira parcela:** será inerente aos serviços de execução única (itens 5 e 6), efetivamente entregues e recebidos, além da parcela anual dos itens 1, 2, 3 e 4, conforme o cronograma contratual. A assinatura do contrato, isoladamente, não autoriza o pagamento. A contratada deverá protocolar o pedido pelo canal institucional indicado pela SETIN, com nota fiscal em nome do TCE/AM, CNPJ nº 05.829.742/0001-48, e descrição do objeto, do contrato, dos quantitativos e do período correspondente.

14.2.4 **Segunda à quinta parcelas:** compreenderão exclusivamente os valores anuais dos itens 1, 2, 3 e 4 efetivamente contratados. O contrato definirá as datas e os documentos de comprovação da cobertura correspondente.

14.2.5 A disponibilização e a comprovação dos direitos de uso de licenças e subscrições serão distinguidas da prestação futura de suporte. Qualquer pagamento que anteceda a execução da obrigação correspondente somente poderá ocorrer se atendidos os requisitos do art. 145, § 1º, da Lei nº 14.133/2021, com justificativa prévia nos autos e previsão expressa no edital, podendo ser exigida garantia adicional. Sem essa instrução, a exigibilidade observará a execução e o atesto, preservada a periodicidade anual.

14.2.6 O pagamento anual não reduz o compromisso da contratada com a cobertura integral de 60 meses. Em caso de antecipação legalmente autorizada e de não execução no prazo contratual, o valor antecipado deverá ser devolvido, na forma do art. 145, § 3º.

14.3 PRAZO DE PAGAMENTO

14.3.1 **O pagamento será efetuado no prazo máximo de até 30 (trinta) dias, contados do recebimento da Nota Fiscal/Fatura, ainda que a proposta divirja dessa condição.**

14.3.2. Considera-se ocorrido o recebimento da nota fiscal ou fatura quando o órgão contratante atestar a execução do objeto do contrato.

14.3.3. No caso de atraso pela Contratante, os valores devidos ao contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice IPCA de correção monetária.

14.4 CONDIÇÕES DE PAGAMENTO

14.4.1 A emissão da Nota Fiscal/Fatura para cobrança será precedida do recebimento da obrigação correspondente e do atesto do fiscal, observadas as condições deste Termo e a hipótese excepcional de antecipação expressamente autorizada nos termos do item 14.2.5.

14.4.2. Quando houver glosa parcial do objeto, à contratante deverá comunicar a empresa para que a mesma declare ciência da glosa e anuência do valor a ser pago.

14.4.3. O setor competente para proceder o pagamento deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

a) a data da emissão;

b) os dados do contrato e do órgão contratante;

c) o período respectivo de execução do contrato, indicando o dia de início e o dia do fim do contrato;

d) o valor a pagar; e

e) eventual destaque do valor de retenções tributárias cabíveis.

14.4.4. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que o contratado providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a contratante;

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

14.4.6. Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta ao SICAF para:

a) verificar a manutenção das condições de habilitação exigidas no edital;

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

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

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

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

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

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

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

14.4.12. O contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, receberá o tratamento tributário legalmente aplicável aos impostos e contribuições abrangidos pelo regime, ressalvadas as hipóteses de retenção previstas na legislação, inclusive quanto ao ISS quando cabível. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

14.4.13 Quaisquer custos adicionais como: impostos, transporte e outros será de responsabilidade da empresa fornecedora vencedora dos itens da licitação.

15. ADEQUAÇÃO ORÇAMENTÁRIA (art. 6º, XXIII, “j”, da Lei nº 14.133/2021)

15.1 As despesas correrão por **recursos específicos** do Orçamento Geral do TCE/AM.

15.2 Dotação orçamentária a indicar na **NE** correspondente ao exercício:

15.2.1 **Gestão/Unidade:** 002101 – Tribunal de Contas do Estado;

15.2.2 **Fonte de Recursos:** 1.500.100 – recursos não vinculados;

15.2.3 Programa de Trabalho: **01.126.0056.2056** (Desenvolvimento e Integração de Sistemas de Controle Informatizados);

15.2.4 Natureza de Despesa: **33.90.40.08** (Serviços Técnicos Profissionais de TIC), para os componentes compatíveis com essa classificação.

15.3 A formação da ata não gera compromisso de execução da totalidade da despesa. A disponibilidade orçamentária e a classificação de cada componente serão confirmadas pela DIORF antes de cada contratação. A aquisição de hardware deverá receber a natureza de despesa própria de bem permanente, conforme orientação contábil, sem imputação automática à rubrica de serviços.

15.4 Para a contratação plurianual, deverão ser observadas as exigências dos arts. 105 e 106 da Lei nº 14.133/2021, inclusive a avaliação de vantagem e a verificação dos créditos e da conveniência da manutenção contratual em cada exercício.

16. DO ESTUDO TÉCNICO

16.1 Integram o planejamento o **Documento de Formalização de Demanda nº 15/2026/DIOTI/SETIN**, o **Estudo Técnico Preliminar – Tecnologia nº 10/2026/DIOTI/SETIN**, a pesquisa de mercado e o cronograma de implementação e migração.

16.2 O ETP fundamenta o registro de até 04 equipamentos, a aquisição inicial de 02 e a previsão condicionada de outro par para o site de contingência, com cobertura de 60 meses e pagamento anual. As especificações técnicas estão consolidadas no Anexo I e o cronograma de atividades no Anexo II.

17. FISCALIZAÇÃO

17.1 A execução dos serviços será objeto de **acompanhamento, controle, fiscalização e avaliação** por representante(s) do TCE-AM, designado(s) por **Portaria**, com atribuições previstas na Lei nº 14.133/2021.

17.1.1 O acompanhamento/fiscalização **não exclui** a responsabilidade da contratada e **não configura solidariedade** com o contratante.

17.2 O contratante poderá **rejeitar, no todo ou em parte**, serviços em desacordo com este Termo.

17.2.1 Havendo objeto rejeitado no recebimento, deverá ser corrigido ou substituído em até **48 (quarenta e oito) horas**, sem ônus. Para incidentes operacionais e reposições durante a garantia, serão observadas também as condições e os níveis de serviço do item 7, inclusive o prazo específico de reposição local contratado.

17.2.2 Descumprido o prazo, configurar-se-á **atraso**, sujeitando a contratada às **sanções**.

18. SUBCONTRATAÇÃO, CESSÃO E/OU TRANSFERÊNCIA

18.1 É **vedada** a **subcontratação**, cessão e/ou transferência **total ou parcial** do objeto. A atuação do fabricante na prestação da garantia e na retaguarda do Centro de Suporte Autorizado, inerente à solução especificada, não afasta a responsabilidade integral da contratada perante o TCE/AM.

19. DOS CRITÉRIOS DE JULGAMENTO DAS PROPOSTAS

19.1 O critério será **menor preço global por lote único**, calculado pela soma dos produtos dos preços unitários pelos quantitativos máximos da ata, considerando a cobertura de **60 meses** dos itens 2, 3 e 4, e os quantitativos máximos dos itens de execução única. Serão observados os preços unitários máximos e a vantagem técnica e econômica do agrupamento.

19.2 Serão desclassificadas as propostas com vícios insanáveis, que não atendam às especificações, com preços inexequíveis ou que permaneçam acima dos limites aceitáveis após negociação, observados o art. 59 da Lei nº 14.133/2021, a possibilidade de diligência e o tratamento sigiloso do

orçamento.

19.3 A proposta deverá discriminar os preços de todos os itens, o valor de cada parcela anual e o valor global dos cinco anos.

20. DOS CASOS OMISSOS

20.1 As omissões, dúvidas e casos não previstos serão dirimidos com base na **Lei nº 14.133/2021** e demais normativos aplicáveis, observado o interesse público e os princípios da Administração.

21. DECLARAÇÃO

21.1 Declaramos que este Termo de Referência se destina à instrução de **Pregão Eletrônico para formação de Ata de Registro de Preços**, pelo critério de **menor preço global em lote único**, para a solução **Palo Alto Networks PA-1420**, com registro de até **04 equipamentos**, aquisição inicial prevista de **02**, subscrições, garantia e suporte por **60 meses** e pagamento anual. A ata terá vigência de **01 ano**, prorrogável por igual período se comprovado o preço vantajoso, observada a Lei nº 14.133/2021.

22. DO FORO

22.1 Fica eleito o **Foro da Comarca de Manaus/AM** para dirimir litígios decorrentes da execução do contrato.

Elaboração do TR:

JOELSON SEABRA LEÃO – Servidor Cedido SEGER

LUCIANE CAVALCANTE LOPES - GTE - Planejamento de Contratações.

ELYNDER BELARMINO – Secretário da SETIN

Página

ANEXO I – ESPECIFICAÇÕES TÉCNICAS E REQUISITOS MÍNIMOS

A.I.1 Appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW) tais como reconhecimento e controle de aplicações, identificação de usuários, prevenção contra ameaças de vírus, spywares e malwares desconhecidos (Zero Day), IPS, filtro de URL e recursos de VPN;

A.I.2 A solução de Firewall de Próxima Geração (NGFW) fornecida deverá acompanhar todas as subscrições de segurança e licenças de software exigidas neste Termo de Referência, devidamente registradas em nome do Órgão Contratante, com prazo de vigência e validade de 60 (sessenta) meses, contados a partir da data de aceitação definitiva do equipamento;

A.I.3 O hardware e software que executem as funcionalidades de proteção de rede devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

A.I.4 O equipamento fornecido deve ser próprio para montagem em rack de 19 polegadas, incluindo kit de fixação ou trilhos, se necessários. Deverão ser fornecidos cabos de alimentação em quantidade suficiente para as duas fontes de cada appliance, com conectores compatíveis com a infraestrutura elétrica ou PDU do órgão.

A.I.5 Deve possuir firewall throughput de, no mínimo, 9,5 Gbps, medido com controle de aplicações App-ID habilitado e tráfego AppMix, conforme documentação pública do fabricante aplicável ao PA-1420;

A.I.6 Deve possuir Threat Prevention throughput de, no mínimo, 6,0 Gbps, medido com App-ID, IPS, antivírus e antispyware habilitados simultaneamente, utilizando tráfego AppMix, conforme datasheet do PA-1420 para PAN-OS 11.2 ou edição posterior que mantenha ou supere esse resultado. O documento comprobatório deverá identificar a versão do PAN-OS e a metodologia de teste utilizada;

A.I.7 Deve suportar, no mínimo, 1.400.000 (um milhão e quatrocentos mil) conexões simultâneas;

A.I.8 Deve suportar, no mínimo, 140.000 (cento e quarenta mil) novas conexões por segundo;

A.I.9 Deve possuir 12 (doze) interfaces RJ45 para dados, sendo 4 (quatro) interfaces 10/100/1000BASE-T e 8 (oito) interfaces multigigabit de 1/2,5/5 GbE;

A.I.10 Das 8 (oito) interfaces RJ45 multigigabit de 1/2,5/5 GbE, pelo menos 4 (quatro) deverão possuir suporte a PoE;

A.I.11 Deve possuir 2 (duas) interfaces SFP de 1 GbE;

A.I.12 Deve possuir 8 (oito) interfaces SFP/SFP+ aptas a operar em 1 ou 10 GbE;

A.I.13 Deve possuir, no mínimo, 1 (uma) interface física de rede de 1 Gbps dedicada para gerenciamento;

A.I.14 Deve possuir uma interface HSCI dedicada de 10 GbE, nativa do appliance, apta a operar como HA2 em configuração active/passive ou como HA2/HA3 em configuração active/active, além de interfaces HA1 dedicadas;

A.I.15 Deve possuir, no mínimo, 1 (uma) interface física do tipo console ou similar;

A.I.16 Deve possuir, no mínimo, 240 (duzentos e quarenta) GB de armazenamento interno para o sistema operacional e registro de logs;

A.I.17 Cada appliance deverá ser entregue com duas fontes de alimentação AC de 450 W instaladas, redundantes, hot-swappable e aptas a operar com compartilhamento de carga. A faixa de entrada deverá ser de 100 a 240 V AC. A falha ou substituição de uma fonte não poderá interromper o funcionamento do equipamento;

A.I.18 Deve suportar, no mínimo, 1.500 (mil e quinhentos) túneis simultâneos de cliente GlobalProtect no total, considerando de forma agregada as conexões SSL, IPsec e IKE XAUTH, devendo ser fornecida a subscrição Prisma Access Agent necessária para os dois appliances do par de alta disponibilidade. Esse quantitativo não se refere a Clientless VPN;

A.I.19 Deve suportar, no mínimo, 200 (duzentos) túneis de VPN IPSEC simultaneamente estando, caso necessário, devidamente licenciado para este fim;

A.I.20 Deve possuir suporte a criação de redes virtuais (VLAN), conforme o padrão IEEE 802.1Q, de, no mínimo, 4.000 (quatro mil) VLANs;

A.I.21 Deve implementar o protocolo LLDP – Link Layer Discovery Protocol;

A.I.22 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);

A.I.23 Deve possuir o recurso de NAT – Network Address Translation nas modalidades de NAT estático 1 para 1, NAT dinâmico 1 para vários e NAT dinâmico vários para vários. Este recurso deve ser aplicado tanto para o endereço de origem quanto para endereço de destino. Deve possuir também NAT64 para tradução entre endereços IPv6 e IPv4 e NPTv6 (Network Prefix Translation) para tradução de um prefixo IPv6 para outro prefixo IPv6 prevenindo problemas de roteamento assimétrico;

A.I.24 Deve suportar a criação de rotas estáticas e os protocolos de roteamento estático e dinâmico RIPv2, OSPFv2 e OSPFv3 incluindo OSPF graceful restart e BGP;

A.I.25 Deve implementar o protocolo ECMP – Equal Cost Multiple Path para balanceamento de carga entre links baseados no hash do endereço IP de origem, no hash do endereço IP de origem e de destino, pela técnica conhecida como round-robin e com base no peso ou prioridade atribuídos a cada link. Deve suportar o balanceamento entre, no mínimo 4 (quatro) links;

A.I.26 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;

A.I.27 Deve possuir o recurso de alta disponibilidade e permitir a configuração nos modos ativo/passivo e ativo/ativo;

A.I.28 Deve implementar controle por políticas/regras de firewall capaz de permitir ou bloquear o tráfego de rede por porta e protocolo, por aplicações, por grupos estáticos de aplicações, por grupos dinâmicos de aplicações baseados em características e comportamento das aplicações, por usuários e grupos de usuários, por endereços IP e faixas de endereços IP e por país de origem e destino do tráfego;

A.I.29 A identificação do país deve ser através do código do país, por exemplo, BR, USA, UK, RUS etc. e através de geolocalização possibilitando a criação de regiões geográficas;

A.I.30 Deve permitir configurar o agendamento das políticas/regras de firewall para habilitar ou desabilitar tais políticas/regras em horários pré-definidos;

A.I.31 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;

A.I.32 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;

A.I.33 Deve possuir a capacidade de reconhecer, no mínimo, 3.000 (três mil) 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 esta uma lista não exaustiva;

A.I.34 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, através da decodificação de protocolos para detectar aplicações encapsuladas dentro do protocolo e identificação através de análise heurística a fim de detectar aplicações através de análise comportamental do tráfego analisado;

A.I.35 Deve permitir a criação de assinaturas personalizadas para o reconhecimento de aplicações proprietárias na própria interface gráfica do equipamento sem a necessidade de intervenção do fabricante;

A.I.36 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;

A.I.37 Deve permitir bloquear sessões TCP que utilizarem variações do three-way-hand-shake como four-way e o five-way split hand shake, prevenindo assim possíveis tráfegos maliciosos;

A.I.38 Deve permitir bloquear conexões que contenham dados no payload dos pacotes TCP SYN e TCP SYN-ACK durante o three-way-hand-shake;

A.I.39 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;

A.I.40 O motor de segurança deve ir além da detecção tradicional baseada estritamente em assinaturas estáticas, possuindo capacidade de análise em linha (inline) baseada em modelos de Aprendizado Profundo (Deep Learning).

A.I.41 As assinaturas deverão poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

A.I.42 Exceções por IP de origem ou de destino deverão ser possíveis nas regras, de forma geral e assinatura a assinatura.

A.I.43 Deverá suportar granularidade nas políticas de IPS Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

A.I.44 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;

A.I.45 Deve possuir a capacidade de detectar e prevenir ameaças em tráfego HTTP/2;

A.I.46 Deve possuir funcionalidade para análise de ameaças de comando e controle desconhecidas, sendo capaz de monitorar e bloquear a comunicação em tempo real através de HTTP, SSL, aplicações desconhecidas de tráfego TCP e UDP;

A.I.47 Deve possuir proteção contra os 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;

A.I.48 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);

A.I.49 A solução de firewall deve possuir funcionalidade para análise de ameaças de comando e controle desconhecidas, sendo capaz de monitorar e bloquear a comunicação em tempo real através de HTTP, SSL, aplicações desconhecidas de tráfego tanto TCP quanto UDP;

A.I.50 A solução de firewall deve possuir funcionalidade para análise de malwares não conhecidos (Malware Zero Day) onde o dispositivo envia o arquivo de forma automática para análise na “cloud” ou em um appliance instalado na rede local onde o arquivo será executado e simulado em um ambiente controlado (sandbox);

A.I.51 Deverá possuir a capacidade de analisar arquivos desconhecidos diretamente no fluxo de dados (inline), utilizando motores de Aprendizado de Máquina (Machine Learning) executados nativamente no plano de dados (data plane) do próprio hardware do firewall.

A.I.52 Caso seja necessário licença de sistema operacional e software para execução de arquivos no ambiente controlado (sandbox) as mesmas devem ser fornecidas em sua totalidade para o seu perfeito funcionamento;

A.I.53 O resultado da análise de malwares não conhecidos deve ter a capacidade de categorizar o arquivo analisado como, no mínimo, um arquivo malicioso, um arquivo não malicioso e um arquivo não malicioso, mas com características indesejáveis que deixam o sistema operacional lento ou que alteram parâmetros do sistema;

A.I.54 A análise de malwares não conhecidos deve ser realizada em arquivos trafegados na internet através dos protocolos HTTP, HTTPS e FTP bem como em arquivos trafegados entre servidores de arquivos utilizando o protocolo SMB. A análise também deve ser realizada em arquivos anexos em e-mails e links HTTP e HTTPS presentes no corpo de e-mails trafegados utilizando os protocolos SMTP e POP3. A análise do link HTTP e HTTPS presente no corpo do e-mail deve identificar se o website é um hospedeiro de exploits ou atividade de phishing;

A.I.55 Suportar a análise com pelo menos 100 (cem) tipos de comportamentos maliciosos para a análise da ameaça não conhecida;

A.I.56 Deve suportar a análise dos arquivos em ambientes controlados (sandbox) com, no mínimo, os sistemas operacionais MS Windows, MacOS e Linux;

A.I.57 A análise de malwares não conhecidos em ambiente controlado (sandbox) deve ser realizada em arquivos tipo executáveis, DLLs, arquivos compactados RAR e 7-ZIP, arquivos do pacote MS Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos PDF, arquivos JAVA (.jar e class), arquivos DMG e PKG, arquivos ELF e arquivos APK;

A.I.58 Deve atualizar a base de assinaturas para bloqueio dos malwares identificados no ambiente controlado (sandbox) dentro de, no máximo, 5 (cinco) minutos;

A.I.59 A solução deverá prover segurança automática para tráfego de DNS, com análise em cloud, provendo aos equipamentos, acesso a assinaturas de DNS, geradas utilizando análise preditiva e aprendizado de máquina, fornecendo dados de domínios maliciosos;

A.I.60 Deverá permitir configuração de categorias de assinaturas de DNS, para possibilitar a criação de políticas de segurança distintas, baseadas em fatores de risco associados com certos tipos de tráfego DNS;

A.I.61 Deverá proteger contra ameaças baseadas em DNS, incluindo aquelas baseadas em DNS dinâmico, domínios registrados recentemente e domínios de phishing;

A.I.62 Deverá proteger contra comunicações de command and control e roubo de dados baseadas em DNS.

A.I.63 O Dispositivo de próxima geração deverá, em sua característica de proteção de DNS, permitir o bloqueio de técnicas de Domain generation algorithms (DGA), evitando assim, que uma máquina contaminada possa tentar estabelecer em um curto espaço de tempo sessão com domínios maliciosos ou inexistentes.

A.I.64 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;

A.I.65 O mecanismo de segurança deve inspecionar o conteúdo e o comportamento das páginas web em tempo real, utilizando Aprendizado de Máquina (Machine Learning), para identificar e bloquear campanhas de phishing e sites maliciosos criados recentemente (just-in-time ou zero-hour), protegendo o usuário no exato momento do clique.

A.I.66 Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

A.I.67 Deverá ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs, Redes e Zonas de segurança;

A.I.68 Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-Directory e base de dados local;

A.I.69 A funcionalidade de filtro URL deve possuir categoria específica para classificar domínios recém registrados com menos de 30 dias;

A.I.70 Deve permitir a criação de categoria de URL customizada permitindo inserir uma lista de URLs específicas;

A.I.71 Deve prover análise em tempo real dos websites acessados pelos usuários realizando a inspeção do seu conteúdo, detectando assim conteúdos que possam ser uma ameaça e realizando a categorização da URL como maliciosa e bloqueando tal URL, mesmo que ela não esteja presente e devidamente categorizada na base de dados de URL da solução;

A.I.72 Permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;

A.I.73 Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

A.I.74 Deve permitir a customização da página de bloqueio exibida ao usuário quando ele tentar realizar um acesso a um website pertencente a uma categoria de URLs bloqueada;

A.I.75 Deve possuir recurso para proteger contra o roubo de credenciais de usuário e senha, identificadas através da integração com o Active Directory, submetidas em sites não corporativos. Deve ser possível definir em quais websites é permitido ou bloqueado o envio das credenciais baseado na categoria de URL a qual o website pertencer. Caso o usuário tente submeter suas credenciais de usuário e senhas pertencentes ao Active Directory em um website não autorizado deve ser exibido no browser web do mesmo uma página de bloqueio informando que o uso de tais credenciais no website específico não está autorizado;

A.I.76 A solução de firewall deve possuir recurso que permita bloquear a transferência de arquivos baseado na extensão dos mesmos e definir por qual aplicação a transferência do arquivo está bloqueada, por exemplo, bloquear a transferência de arquivos .exe através de web browser. Deve permitir bloquear, no mínimo, arquivo com as extensões .exe, .bat, .dll, .pif e .torrent;

A.I.77 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;

A.I.78 A integração com MS Active Directory para identificação dos usuários da rede deve ser realizada sem a necessidade de instalação de um agente no Controlador de Domínio e nem nas estações dos usuários;

A.I.79 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;

A.I.80 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 e SSL – Secure Sockets Layer;

A.I.81 O recurso de VPN IPSec deve suportar os algoritmos de criptografia 3DES, AES 128, AES 192 e AES 256, os algoritmos de autenticação MD5, SHA-1, SHA-256, SHA-384 e SHA-512, o algoritmo IKEv1 e IKEv2 e os algoritmos de troca de chaves Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 e Grupo 14 e suportar também a autenticação através de certificados IKE PKI;

A.I.82 O recurso de VPN SSL deve permitir que o usuário remoto se conecte através de um software cliente de VPN instalado no sistema operacional do equipamento do usuário sendo possível a atribuição de endereços IP fixos e atribuição de DNS ao mesmo;

A.I.83 Deve suportar a autenticação dos usuários remotos que se conectam à VPN via LDAP, MS Active Directory, TACACS+, RADIUS, SAML e através de base de usuários local no equipamento da solução de firewall. Deve suportar também a autenticação via certificado e OTP – One Time Password;

A.I.84 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, MS Windows 11, MacOS e Linux e para instalação em dispositivos móveis Android e IOS;

A.I.85 O recurso de VPN SSL deve possuir mecanismo de checagem da conformidade do computador do usuário remoto e a checagem deve permitir verificar, no mínimo, as informações de qual sistema operacional e patches estão instalados, se o antivírus está instalado e ativo no computador, se o firewall está instalado e ativo no computador, se o disco está criptografado, se o agente de DLP – Data Loss Prevention está instalado e ativo, informações de chaves de registro e processos ativos no computador;

A.I.86 Deve ser possível criar perfis customizados de conformidade com, no mínimo, as mesmas informações obtidas pelo mecanismo de checagem da conformidade do computador do usuário remoto. Tais perfis devem ser utilizados para assegurar que apenas computadores de usuários remotos que atendem aos requisitos solicitados nos perfis customizados possam ter acesso através da VPN aos dados e sistemas hospedados na rede interna do órgão;

A.I.87 A solução de firewall deve possuir console de gerenciamento do equipamento acessada através de interface gráfica web 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;

A.I.88 Deve suportar a autenticação dos usuários administradores que se conectam à interface de gerenciamento do equipamento via LDAP, MS Active Directory, RADIUS e através de base de usuários local no equipamento da solução de firewall;

A.I.89 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;

A.I.90 Deve permitir realizar o backup das configurações do equipamento e a restauração da configuração salva através de interface de gerenciamento;

A.I.91 A interface de gerenciamento do equipamento deve possuir recurso para análise das políticas indicando, quando houver, regras que ofusquem, conflitem ou sobreponham outras regras (shadowing) e quais objetos não estão sendo utilizados, para avaliação de elementos dispensáveis, permitindo assim, a higienização gradual das regras e seus respectivos elementos. Deve possuir também recurso para análise das políticas indicando, quando houver, regras baseadas em porta e protocolo, permitindo a conversão dela para uma regra baseada em aplicação, melhorando assim o controle do tráfego e a segurança do ambiente. É permitido o uso de appliance externo para realização da análise das políticas, devendo o mesmo ser fornecido em conjunto com a solução de firewall e estar devidamente licenciado;

A.I.92 Deve ser possível através de interface de gerenciamento do equipamento a geração de relatórios tais como um resumo gráfico das aplicações utilizadas e ameaças vistas, principais aplicações por utilização de largura de banda, atividades de um usuário ou grupo de usuário específicos incluindo aplicações e URLs acessadas e permitir a criação de relatórios personalizados;

A.I.93 Deve ser possível gerar relatório de visibilidade e uso das aplicações do tipo SaaS – Software as a Service mostrando os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso a aplicação SaaS e o consumo da aplicação SaaS pelo usuário;

A.I.94 Deve ser exibida na interface gráfica de gerenciamento do equipamento informações em tempo real, atualizadas de forma automática a cada 1 (um) minuto, as principais aplicações acessadas, o risco das principais aplicações, número de sessões simultâneas, status das interfaces de rede e uso de CPU;

A.I.95 Deve ser possível configurar o envio de alertas do sistema via e-mail;

A.I.96 Deve suportar o monitoramento via SNMPv3;

A.I.97 O sistema operacional a ser instalado no equipamento que compõe a solução deverá ser fornecido em sua versão mais atualizada, não sendo aceito sistema operacional de uso genérico;

A.I.98 Por cada equipamento que compõe a solução de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;

A.I.99 Na data do certame, nenhum dos equipamentos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

A.I.100 A solução de firewall deve possuir garantia pelo período de 60 (sessenta) meses, compreendendo a reposição de peças/equipamentos, atualizações do sistema operacional do equipamento e demais software e das assinaturas de proteção da solução.

A.I.101 Durante o período de vigência do contrato de garantia, todos os componentes da solução de firewall, incluindo hardware, PAN-OS, subscrições, aplicativo cliente de VPN e demais itens necessários ao funcionamento, deverão estar cobertos pelo suporte do Centro de Suporte Autorizado (ASC), com retaguarda da Palo Alto Networks.

ANEXO II – CRONOGRAMA DE IMPLEMENTAÇÃO E MIGRAÇÃO

O cronograma contempla as atividades do planejamento técnico. A contratada deverá convertê-lo em programação datada, previamente aprovada pela SETIN, incluindo entrega, início e fim da implantação, capacitação, responsáveis e janelas de mudança. A mesma sequência aplica-se ao segundo par, caso contratado, com as adaptações necessárias ao site de contingência.

Etapa	Atividades	Hor
1. Início e planejamento	Reunião inicial; definição de responsáveis, escopo e janela; levantamento da arquitetura, interfaces, VLANs, roteamento, NAT, VPNs, serviços e políticas	
2. Avaliação da solução atual	Análise de regras; identificação de objetos, NAT e VPNs a migrar; revisão de regras obsoletas, duplicadas ou conflitantes; estratégia de migração	
3. Preparação do ambiente	Instalação física e conexão; atualização e validação do PAN-OS; configuração de interfaces, zonas, VLANs, roteadores virtuais e alta disponibilidade	
4. Migração da configuração	Criação/importação de objetos; regras de segurança; NAT; rotas; VPNs; acessos administrativos e perfis de segurança	
5. Validação prévia	Revisão da configuração; validação de objetos, regras, NAT e roteamento; testes controlados; plano de mudança e reversão	
6. Entrada em produção	Backup; janela de mudança; ativação em produção; testes de conectividade, aplicações críticas, VPNs, NAT e acessos publicados	
7. Estabilização	Monitoramento; ajustes de regras e políticas; validação de logs, Threat Prevention e demais subscrições	
8. Documentação e encerramento	Documentação da configuração e do ambiente implantado; transferência de conhecimento; reunião de encerramento	
TOTAL	**Esforço técnico estimado por implantação:**	

A capacitação do item 6 da tabela 4.1 terá programação própria, com carga horária mínima de 40 horas, conforme o item 4.1.4. As 124 horas acima não incluem o tempo de fornecimento físico dos equipamentos nem substituem a fixação dos prazos contratuais de entrega e conclusão.

Elaboração do TR:

JOELSON SEABRA LEÃO

SERVIDOR CEDIDO - ASSESSORIA SEGER

Revisão do TR:

ADRIA OLIVEIRA DA SILVA

CHEFE DE INFRAESTRUTURA EM TECNOLOGIA DA INFORMAÇÃO

CELSO RICARDO LIMA MARTINS

DIRETOR DE OPERAÇÕES EM TECNOLOGIA DA INFORMAÇÃO

LUCIANE CAVALCANTE LOPES

GTE-PLANEJAMENTO DE CONTRATAÇÕES PÚBLICAS

APROVAÇÃO DA AUTORIDADE SUPERIOR:

APROVO o presente TERMO DE REFERÊNCIA, pois constatei que atende às condições previstas na Lei nº 14.133/2021 e legislação em vigor.

ANTÔNIO CARLOS SOUZA DA ROSA JUNIOR
SECRETÁRIO-GERAL DE ADMINISTRAÇÃO

Documento assinado eletronicamente por **JOELSON SEABRA LEAO**, **Assessor(a)**, em 03/11/2026, às 11:36, conforme horário oficial de Manaus, com fundamento na Resolução n.º 07, de 30 de agosto de 2022, publicada na Edição n.º 2880, Pag. 18, do Diário Oficial Eletrônico (D.O.E.) do Tribunal de Contas do Estado do Amazonas.

Documento assinado eletronicamente por **Luciane Cavalcante Lopes**, **Chefe de Planejamento de Contratações Públicas**, em 03/11/2026, às 20:08, conforme horário oficial de Manaus, com fundamento na Resolução n.º 07, de 30 de agosto de 2022, publicada na Edição n.º 2880, Pag. 18, do Diário Oficial Eletrônico (D.O.E.) do Tribunal de Contas do Estado do Amazonas.

A autenticidade deste documento pode ser conferida no site https://sei.tce.am.gov.br/sei/autenticar, informando o código verificador **0934491** e o código CRC **D599A6CE**.

Referência: Processo nº 005280/2026 SEI nº 0934491