TERMO DE REFERÊNCIA

1. OBJETO

1.1. Registro de Preços para eventual renovação do suporte e das licenças do cluster de equipamentos de Next-Generation Firewall, assim como expansão da solução de firewall para as unidades descentralizadas do Tribunal de Justiça do Estado do Amazonas (TJAM), compreendendo suporte técnico e garantia pelo período de 60 meses, incluindo serviços de instalação, configuração e treinamento oficial do fabricante.

2. JUSTIFICATIVA

2.1. MOTIVAÇÃO

2.1.1. O TJAM utiliza o método de proteção em camadas de segurança. Este método consiste em criar várias camadas de proteção distintas e complementares, sendo que cada camada atua de forma especializada em algum componente de segurança. Uma das principais camadas de proteção em um ambiente de TI é o equipamento de firewall, ativo que possui a capacidade de inspecionar, controlar e bloquear o tráfego proveniente da Internet com destino aos sistemas e serviços do TJAM, sendo também possível aplicar políticas e restrições de acessos inter-redes e controlar os acessos dos usuários internos com destino à Internet;

2.1.2. A solução atual possui contrato de suporte técnico especializado e garantia, bem como módulos de subscrições de IPS (*Intrusion Prevention System*), Filtro de conteúdo Web, Análise de Malware e software de gerenciamento de plataforma de segurança, que expira em Novembro/2023. Destaca-se que uma solução de segurança cibernética somente se sustenta se estiver plenamente atualizada, uma vez que as funcionalidades das ferramentas de segurança fazem uso de recursos de inteligência de reputação, providos através das subscrições e fornecidos pelo fabricante da plataforma de segurança da solução. Dessa forma, muitas atividades e ações podem ser automatizadas, reduzindo o esforço da equipe técnica e também diminuindo possíveis falhas de operação que podem impactar na disponibilidade e estabilidade do ambiente;

2.1.3. Devido a complexidade das soluções de segurança, faz-se necessário manter um suporte técnico especializado, 24x7, com o objetivo de poder acionar um suporte técnico, obter recomendações de melhores práticas e assessoramento para o funcionamento da plataforma de solução de segurança. Além disso, a garantia é fundamental para manter contratos de substituição de peças e equipamentos durante a vigência do contrato;

2.1.4. Considerando que o TJAM já utilizada há mais de 05 anos a plataforma de solução de segurança da fabricante Palo Alto Networks, que vem mantendo a estabilidade, pleno funcionamento e a confiabilidade em um ambiente complexo como a infraestrutura do TJAM, busca-se também expandir as soluções de segurança integradas na plataforma para todas as unidades descentralizadas da capital e do interior do Judiciário Amazonense, bem como suportar o aumento das capacidades operacionais necessários para acompanhar as cargas de trabalho demandados pelos equipamentos do núcleo da rede;

2.1.5. Com os recursos adquiridos, será possível modificar a arquitetura atual e realizar a expansão da tecnologia de firewall do TJAM para as unidades descentralizadas, equipando-as com *apliances* Palo Alto de menor capacidade, mas com recursos suficientes para permitir gerenciamento centralizado através do Panorama e ainda interconexão de múltiplos links com a tecnologia SD-WAN;

2.1.6. As motivações também estão alinhadas com as recomendações de diferentes órgãos e instruções normativas à respeito da adoção de controles gerais de segurança da informação, dentre os quais destacam-se:

2.1.6.1. O decreto 10.222, de 5 de fevereiro de 2020, que dispõe sobre a Estratégia Nacional de Segurança Cibernética, cita com um dos seus objetivos o aumento da resiliência brasileira às ameaças cibernética elevando principalmente o nível de proteção do Governo.

> “Aperfeiçoar e manter atualizados os sistemas informacionais, as infraestruturas e os sistemas de comunicação dos órgãos públicos, em relação aos requisitos de segurança cibernética, adotando que abordem iniciativas integradoras”

2.1.6.2. A Lei 13.709, de 14 de agosto de 2018, intitulada como a Lei Geral de Proteção de Dados Pessoais (LGPD), em seu artigo 46 cita que:

> “os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito”

2.1.6.3. A Resolução 370 de 28/01/2021, Estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), onde orientada em seu preâmbulo pelos objetivos dos seguintes componentes:

> “Objetivo 7: Aprimorar a Segurança da Informação e a Gestão de Dados”.

2.1.6.4. Na Resolução 396 de 07/06/2021 do CNJ, que institui a Instituir a Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário (ENSEC-PJ) no âmbito dos órgãos do Poder Judiciário, à exceção do Supremo Tribunal Federal (STF), destaca-se o artigo:

> "Art. 9º São ações da ENSEC-PJ:
>
> I - fortalecer as ações de governança cibernética;
>
> II - elevar o nível de segurança das infraestruturas críticas;
>
> III - estabelecer rede de cooperação do Judiciário para a segurança cibernética;
>
> IV - estabelecer modelo centralizado de governança cibernética nacional."

2.1.7. A renovação das subscrições e a expansão da solução de firewall para as unidades descentralizadas é a alternativa mais apropriada para o TJAM, permitindo que o Tribunal mantenha toda as barreiras de proteção já implementadas e proporcione um incremento nessas barreiras com a expansão desses recursos de proteção contra os ataques cibernéticos que crescem assustadoramente e que atingem diversos outros órgãos e tribunais, como por exemplo, os ataques ocorridos no Supremo Tribunal Federal (2021), Superior Tribunal de Justiça (2021), Tribunal de Justiça do Estado do Rio Grande do Sul (2021), Tribunal de Justiça do Estado do Amazonas (2021), TRT 4 Região (2021), TRF 3 Região (2022), TRT-ES (2022), Tribunal de Contas do Ceará (2022), Justiça Federal de Pernambuco (2022), entre outros;

2.1.8. Além das razões apresentadas, existem as necessidades em manter a eficácia, integração e a qualidade da plataforma de segurança em um ambiente de TI complexo como o do TJAM, bem como reduzir possíveis impactos gerados pela indisponibilidade dos serviços e sistemas de TIC e também evitar a reimplementação das barreiras de seguranças já em operação do TJAM.

2.2. OBJETIVOS

2.2.1. Esta contratação tem o objetivo de aumentar a estabilidade e a confiabilidade da solução de Firewall existente no TJAM, que atua na proteção da borda de Internet, na proteção dos ativos de rede do datacenter, bem como permitir a expansão da tecnologia de firewall do TJAM para as unidades descentralizadas, permitindo gerenciamento centralizado através do Panorama e ainda interconexão de múltiplos links com a tecnologia SD-WAN;

2.2.2. Busca-se também preservar os investimentos realizados no ambiente do TJAM, pois durante o período de vigência dos equipamentos o corpo técnico da SETIC adquiriu amplo conhecimento e experiencia na solução de segurança atual, permitindo o desenvolvimento de projetos específicos para levar segurança aos usuários internos e remotos do TJAM.

2.3. BENEFÍCIOS

2.3.1. Manter a estabilidade, confiabilidade e proteção da segurança do tráfego de perímetro e da borda de acesso à Internet, através da renovação da solução de segurança atual que se encontra em pleno funcionamento;

2.3.2. Expandir os recursos de segurança da tecnologia de firewall do TJAM para as unidades descentralizadas, equipando-as com *apliances* Palo Alto de menor capacidade, mas com recursos suficientes para permitir gerenciamento centralizado através do Panorama e ainda interconexão de múltiplos links com a tecnologia SD-WAN;

2.3.3. Introduzir o conceito de Zero Trust na arquitetura nas unidades descentralizadas do TJAM, permitindo que todo o Judiciário Amazonense esteja atualizado com as melhores práticas e referências quanto à segurança da informação;

2.3.4. Dispor de equipamentos e soluções com tecnologias e recursos atualizados para o enfrentamento dos riscos de segurança no ambiente de TI;

2.3.5. Prover a garantia da solução de segurança em firewall com eficaz substituição de peças dos equipamentos, para que seja mantida a alta disponibilidade das operações;

2.3.6. Garantir o nível de suporte técnico necessário para atender um ambiente corporativo complexo e robusto como o do TJAM;

2.3.7. Aperfeiçoar a detecção e a diminuição do tempo respostas às ameaças cibernéticas contra o ambiente do TJAM;

2.3.8. Obter suporte adequado do fabricante quanto às necessidade de aperfeiçoamento, adoção das melhores práticas na solução de segurança e resoluções de problemas.

2.4. ALINHAMENTO ESTRATÉGICO

2.4.1. Entende-se que a presente aquisição compartilha dos objetivos pretendidos no Plano Diretor de Tecnologia da Informação e Comunicação- PDTIC, referente ao biênio 2023-2024, do TJAM;

2.4.1.1. Perspectiva: Processos Internos

2.4.1.2. Objetivo Estratégico: Aperfeiçoamento administrativa e da governança judiciária

2.4.1.3. Iniciativa Estratégica: Renovação das Licenças do Palo Alto

2.4.1.4. Descrição: Contratação de empresa especializada para licenciamento das *appliances* Palo Alto

3. FUNDAMENTO LEGAL

3.1. Não há legislação aplicável especificamente ao objeto licitado, além das que regem o processo licitatório e que já foram identificadas no Estudo Técnico Preliminar - a saber: Lei nº. 8.666/93, de 21 de junho de 1993; Lei n°10.520, de 17 de julho de 2002 e Resolução nº 25/2019 do TJAM.

4. DEFINIÇÕES E TERMINOLOGIA

4.1. Para fins deste Termo de Referência (TR):

4.1.1. TJAM: o Tribunal de Justiça do Amazonas será denominado simplesmente de “TJAM”;

4.1.2. SETIC: a Secretaria de Tecnologia da Informação e Comunicação será denominada simplesmente de “SETIC”;

4.1.3. EMPRESA CONTRATADA: a(s) empresa(s) vencedora(s) do processo licitatório e responsável(eis) pelo objeto será denominada simplesmente de “CONTRATADA”;

4.1.4. PRODUTO: Objeto do Termo de Referência, seja ele hardware, software, acessório, periférico ou consumível poderá será denominado simplesmente de "produto";

4.1.5. HORÁRIO REGIMENTAL DO TJAM: período compreendido entre 8h e 14h, de segunda a sexta-feira, excluídos os feriados, será denominado simplesmente de "HORÁRIO REGIMENTAL DO TJAM";

4.1.6. TIC: a Tecnologia da Informação e Comunicação será denominada simplesmente de "TIC";

4.1.7. SD-WAN: a sigla para se referir ao termo "Software-Defined Wide Area Network". Trata-se de uma abordagem onde as definições de tráfego são controladas por software de forma a se criar uma sobreposição virtual para permitir a conectividade no âmbito de redes WAN.

5. DO REGISTRO DE PREÇOS

5.1. O procedimento para a aquisição/contratação pretendida será regido pelo Sistema de Registro de Preços.

6. ESPECIFICAÇÃO DO OBJETO

6.1. Contexto:

6.1.1. A atual solução de Firewall conta apenas com dois equipamentos, que possuem subscrição de suporte técnico especializado e garantia, bem como módulos de Prevenção a Ameaças, Filtro de URL e Análise de Malware, que expiram totalmente em fevereiro/2024.

6.1.2. Além disso, conforme verificado no item 2.1.4 deste Termo de Referência, faz-se necessário expandir essa solução para todas as unidades descentralizadas da capital e do interior do Judiciário Amazonense;

6.1.3. Sendo assim, o quadro abaixo possui itens de renovação (1 a 4) e de expansão (5 a 18) da atual solução:

Renovação e expansão de solução de firewall para o ambiente de datacenter e unidades descentralizadas		
ITEM	**CÓDIGO SIASG**	**ESPECIFICAÇÕES**
1	27502	Subscrição de Prevenção a Ameaças para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.
2	27502	Subscrição de Filtro de URL para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.
3	27502	Subscrição de Análise de Malware para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.
4	27340	Garantia da Solução de Plataforma de Segurança Palo Alto Networks PA-5220, com suporte Premium oficial Palo Alto Networks 24x7 em Alta Disponibilidade, pelo período de 60 meses.
5	481646	Firewall Palo Alto PA-410
6	27502	Subscrição CORE SECURITY SUBSCRIPTION BUNDLE (ADVANCED THREAT PREVENTION, ADVANCED URL FILTERING, ADVANCED WILDFIRE, DNS SECURITY AND SD-WAN) para PA-410, pelo período de 60 meses.
7	27340	Garantia da Solução de Plataforma de Segurança Palo Alto Networks PA-410, com suporte Premium oficial Palo Alto Networks 24x7, pelo período de 60 meses.
8	27502	Subscrição de Licença de Gerência Centralizada com suporte para 100 dispositivos Palo Alto Networks, pelo período de 60 meses.
9	27340	Garantia da Solução de Panorama, com suporte Premium oficial Palo Alto Networks 24x7, pelo período de 60 meses.
10	27502	Subscrição de DNS Seguro para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.
11	27502	Subscrição de SD-WAN Seguro para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.
12	27340	Serviço de instalação das soluções de Next-Generation Firewall Palo Alto Networks PA-410 e PA-5410.
13	21172	Treinamento oficial do fabricante remoto, em língua portuguesa, com disponibilização de voucher para certificação de administração da solução Palo Alto.
14	27502	Subscrição de GlobalProtect para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.
15	481646	Firewall Palo Alto PA-5410
16	27502	Subscrição CORE SECURITY SUBSCRIPTION BUNDLE (ADVANCED THREAT PREVENTION, ADVANCED URL FILTERING, ADVANCED WILDFIRE, DNS SECURITY AND SD-WAN) para PA-5410, pelo período de 60 meses.
17	27340	Garantia da Solução de Plataforma de Segurança Palo Alto Networks PA-5410, com suporte Premium oficial Palo Alto Networks 24x7, pelo período de 60 meses.
18	27502	Subscrição de GlobalProtect para solução de Plataforma de Segurança Palo Alto Networks PA-5410, pelo período de 60 meses.

6.1.4. Os serviços deverão ser fornecidos por empresa única, sob o regime de menor preço global, em conformidade com especificado neste TR, responsabilizando-se por fornecer todo e qualquer componente necessário ao pleno estado de funcionamento do serviço.

6.2. Funcionalidades gerais:

6.2.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;
6.2.2. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
6.2.3. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
6.2.4. O hardware e software que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;
6.2.5. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:
6.2.6. Agregação de links 802.3ad e LACP;
6.2.7. Policy based routing ou policy based forwarding;
6.2.8. Roteamento multicast (PIM-SM);
6.2.9. DHCP Relay;
6.2.10. DHCP Server;
6.2.11. Jumbo Frames;
6.2.12. Suporte a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3;
6.2.13. Suportar sub-interfaces ethernet logicas;
6.2.14. Deve suportar os seguintes tipos de NAT:
6.2.15. Nat dinâmico (Many-to-1);

6.2.16. Nat dinâmico (Many-to-Many);
6.2.17. Nat estático (1-to-1);
6.2.18. NAT estático (Many-to-Many);
6.2.19. Nat estático bidirecional 1-to-1;
6.2.20. Tradução de porta (PAT);
6.2.21. NAT de Origem;
6.2.22. NAT de Destino;
6.2.23. Suportar NAT de Origem e NAT de Destino simultaneamente;
6.2.24. Deve implementar Network Prefix Translation (NPTv6);
6.2.25. Enviar log para sistemas de monitoração externos;
6.2.26. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
6.2.27. Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;
6.2.28. Proteção contra anti-spoofing;
6.2.29. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
6.2.30. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
6.2.31. Suportar a OSPF graceful restart;
6.2.32. Deve suportar o protocolo MP-BGP (Multiprotocol BGP) permitindo que o firewall possa anunciar rotas multicast para IPv4 e rotas unicast para IPv6;
6.2.33. Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (l2) e camada 3 (l3);
6.2.34. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
6.2.35. Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
6.2.36. Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
6.2.37. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
6.2.38. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:
6.2.39. Em modo transparente;
6.2.40. Em layer 3;
6.2.41. A configuração em alta disponibilidade deve sincronizar:
6.2.41.1. Sessões;
6.2.41.2. Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;
6.2.41.3. Certificados de-criptografados;
6.2.41.4. Associações de Segurança das VPNs;
6.2.41.5. Tabelas FIB;
6.2.41.6. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.

6.3. Funcionalidades específicas:
6.3.1. Subscrição de Prevenção a Ameaças para solução de Plataforma de Segurança Palo Alto Networks
6.3.1.1. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
6.3.1.2. Deve ter a capacidade de bloquear ameaças desconhecidas em tempo real;
6.3.1.3. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.
6.3.1.4. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
6.3.1.5. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
6.3.1.6. Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura;
6.3.1.7. Deve permitir o bloqueio de vulnerabilidades.
6.3.1.8. Deve permitir o bloqueio de exploits conhecidos.
6.3.1.9. Deve incluir proteção contra ataques de negação de serviços.
6.3.1.10. Deverá possuir os seguintes mecanismos de inspeção de IPS:
6.3.1.11. Análise de padrões de estado de conexões;
6.3.1.12. Análise de decodificação de protocolo;
6.3.1.13. Análise para detecção de anomalias de protocolo;
6.3.1.14. Análise heurística;
6.3.1.15. IP Defragmentation;
6.3.1.16. Remontagem de pacotes de TCP;
6.3.1.17. Bloqueio de pacotes malformados.

6.3.1.18. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc;
6.3.1.19. Detectar e bloquear a origem de portscans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização;
6.3.1.20. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
6.3.1.21. Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;
6.3.1.22. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
6.3.1.23. Possuir assinaturas para bloqueio de ataques de buffer overflow;
6.3.1.24. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
6.3.1.25. Identificar e bloquear comunicação com botnets;
6.3.1.26. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
6.3.1.27. O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
6.3.1.28. Deve suportar a captura de pacotes (PCAP), por assinatura de Malware e aplicação;
6.3.1.29. Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
6.3.1.30. Os eventos devem identificar o país de onde partiu a ameaça;
6.3.1.31. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.
6.3.1.32. Proteção contra downloads involuntários usando HTTP de arquivos executáveis. maliciosos.
6.3.1.33. Rastreamento de vírus em pdf.
6.3.1.34. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.).
6.3.2. Subscrição de Filtro de URL para solução de Plataforma de Segurança Palo Alto Networks
6.3.2.1. Deve suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
6.3.2.2. Deve possuir a função de exclusão de URLs do bloqueio;
6.3.2.3. Deve permitir a customização de página de bloqueio;
6.3.2.4. Deverá permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);
6.3.2.5. Deve permitir controlar o envio de credenciais corporativas somente para categorias de URLs permitidas;
6.3.2.6. Deve prover análise em tempo real de páginas maliciosas e dessa forma permitir a proteção em tempo real antes mesmo da atualização das bases de dados de URLs;
6.3.3. Subscrição de Análise de Malware para solução de Plataforma de Segurança Palo Alto Networks
6.3.3.1. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;
6.3.3.2. Deve ser capaz de enviar para análise, arquivos tipo Executáveis, DLLs, Arquivos de Código e MSI;
6.3.3.3. Deve ser capaz de analisar arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows, Linux, MacOS e Android;
6.3.3.4. A solução deve possuir a capacidade de extrair e analisar em sand-box links (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3. Deve ser gerado um relatório caso a abertura do link pela sand-box o identifique como site hospedeiro de exploits;
6.3.3.5. A análise de links em sand-box deve ser capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução;
6.3.3.6. Deve permitir exportar o resultado das análises de malwares de dia zero em PDF e CSV a partir da própria interface de gerência;
6.3.3.7. Deve permitir o download dos malwares identificados a partir da própria interface de gerência;
6.3.3.8. Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;
6.3.3.9. Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia zero a partir da própria interface de gerência.
6.3.3.10. Caso sejam necessárias licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sand-box), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;
6.3.3.11. Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;
6.3.3.12. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), Android APKs, MacOS (mach-O, DMG e PKG), Linux (ELF), RAR e 7-ZIP no ambiente de sandbox;

6.3.3.13. Deve atualizar a base com assinaturas para bloqueio dos malwares identificados em sand-box com frequência de, pelo menos, 5 minutos;
6.3.3.14. Permitir o envio de arquivos e links para análise no ambiente controlado de forma automática via API.
6.3.3.15. Deve permitir o envio para análise em sand-box de malwares bloqueados pelo antivírus da solução;
6.3.3.16. A solução deve analisar os arquivos do tipo malware em bare metal para evitar técnicas de evasão. Caso não possua essa funcionalidade será permitido a integração com ferramentas que executam esta função.
6.3.3.17. Deve prevenir contra-ataques sem arquivo buscando por atividade maliciosa em pelo menos nas seguintes linguagens de scripts: Powershell e Javascript.
6.3.4. Firewall Palo Alto PA-410
6.3.4.1. Deve possuir throughput de, no mínimo, 1 (um) Gbps com a funcionalidade de controle de aplicação para todas as assinaturas que o fabricante possuir;
6.3.4.2. Deve possuir throughput de, no mínimo, 650 (Seiscentos e cinquenta) Mbps com as funcionalidades de controle de aplicação, IPS, Antivírus e Anti-Spyware habilitadas simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os throughput aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real;
6.3.4.3. Deve suportar, no mínimo, 60.000(Sessenta mil) conexões simultâneas;
6.3.4.4. Deve suportar, no mínimo, 10.000 (dez mil) novas conexões por segundo;
6.3.4.5. Deve possuir, no mínimo, 6 (seis) interfaces físicas de rede de 1Gbps do tipo RJ-45;
6.3.4.6. Deve possuir, no mínimo, 1 (uma) interface física de rede de 1 Gbps dedicada para gerenciamento out of band, ou seja, não será permitida a utilização de interfaces genéricas e não dedicadas para o fim;
6.3.4.7. Deve possuir, no mínimo, 1 (uma) interface física do tipo console ou similar;
6.3.4.8. Deve possuir armazenamento interno para registro de logs;
6.3.4.9. Deve possuir fonte de alimentação elétrica capaz de operar entre 120 a 240 VAC;
6.3.4.10. Deve suportar, no mínimo, 300 (trezentos) túneis de VPN IPSEC Gateway to Gateway simultaneamente estando, caso necessário, devidamente licenciado para este fim;

6.3.5. Subscrição de DNS Seguro para solução de Plataforma de Segurança Palo Alto Networks

6.3.5.1. 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;
6.3.5.2. 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;
6.3.5.3. Deverá proteger contra ameaças baseadas em DNS, incluindo aquelas baseadas em DNS dinâmico, domínios registrados recentemente e domínios de phishing;
6.3.5.4. Deverá proteger contra comunicações de command and control e roubo de dados baseadas em DNS.
6.3.5.5. 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.

6.3.6. Subscrição de SD-WAN Seguro para solução de Plataforma de Segurança Palo Alto Networks

6.3.6.1. Deverá operacionalizar no mínimo os seguintes critérios de SD-WAN:
6.3.6.2. As configurações de profiles de SD-WAN deverão partir de um ponto central permitindo alteração e criação dos elementos primordiais para o funcionamento da solução, assim flexibilizando a configuração inicial e suas devidas manutenções;
6.3.6.3. A solução deverá permitir operar em caráter de diagrama hub-spoke;
6.3.6.4. Os dispositivos deverão ter a capacidade de exibir impactos por aplicação;
6.3.6.5. A solução deverá permitir ao administrador métricas de utilização de banda por circuito disponível e desta forma exibir no mínimo itens em porcentagem ou contadores, jitter, latência e perda de pacote;
6.3.6.6. O dispositivo deverá compreender o que está causando desempenho de degradação para as aplicações e serviços ativos e assim garantir que a experiência do usuário sofra o menor impacto possível;
6.3.6.7. O SD-WAN deverá suportar os seguintes tipos de conexões WAN: ADSL/DSL, Cable Modem com Ethernet ou fibra, LTE /3G/4G/5G, MPLS, Link de rádio e Link satélite desde que a sua terminação permita conectividade com interfaces ethernet.
6.3.6.8. A solução deverá ter inteligência para executar no mínimo as seguintes lógicas de operação:
6.3.6.9. Distribuição de tráfego por prioridade de circuito, circuitos exclusivos de contingenciamento em 3G/4G/5G deverão ser utilizados apenas em caso de falha geral dos circuitos ADSL/MPLS;
6.3.6.10. Distribuição de tráfego de acordo com métricas definidas por origem e destino, o dispositivo

deverá permitir ao administrador criar perfis com base em latência, jitter ou perda de pacotes para que uma vez que estes limites sejam atingidos o dispositivo possa manter a conexão por circuitos que apresente resultados abaixo dos limites definidos;
6.3.6.11. Distribuição de tráfego com balanceamento de sessão entre os circuitos existentes;
6.3.6.12. Distribuição orientada a qualidade, o dispositivo deverá validar o melhor caminho disponível e utilizar-se deste path para manter sessões ativas, caso o melhor caminho entre em degradação por fatores anômalos o dispositivo deverá entender estes fatores e distribuir para os demais circuitos existentes.
6.3.6.13. A Solução de SD-WAN deverá desempenhar a função de Forward Error Correlation (FEC).
6.3.6.14. A Solução de SD-WAN deverá desempenhar a função de Packet Duplication (PD) permitindo encaminhar o pacote por mais de um circuito para em casos de falhas não haver retransmissão.
6.3.6.15. Os dispositivos deverão suportar a funcionalidade de ZTP (Zero Touch Provisioning) para que assim, inseridos nas estruturas remotas, possam buscar automaticamente por suas configurações, com o objetivo de facilitar a instalação nas unidades remotas ou a troca de um dispositivo defeituoso.
6.3.7. Subscrição de GlobalProtect para solução de Plataforma de Segurança Palo Alto Networks

6.3.7.1. Suportar VPN Site-to-Site e Cliente-To-Site;
6.3.7.2. Suportar IPSec VPN;
6.3.7.3. Suportar SSL VPN;
6.3.7.4. A VPN IPSEc deve suportar:
6.3.7.4.1. 3DES;
6.3.7.4.2. Autenticação MD5 e SHA-1;
6.3.7.4.3. Diffie-Hellman Group 1 , Group 2, Group 5 e Group 14;
6.3.7.4.4. Algoritmo Internet Key Exchange (IKEv1 e v2);
6.3.7.4.5. AES 128, 192 e 256 (Advanced Encryption Standard)
6.3.7.4.6. Autenticação via certificado IKE PKI.
6.3.7.5. Deve possuir interoperabilidade com os seguintes fabricantes:
6.3.7.5.1. Cisco;
6.3.7.5.2. Checkpoint;
6.3.7.5.3. Juniper;
6.3.7.5.4. Palo Alto Networks;
6.3.7.5.5. Fortinet;
6.3.7.5.6. Sonic Wall;
6.3.7.6. Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de troubleshooting;
6.3.7.7. A VPN SSL deve suportar:
6.3.7.7.1. O usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
6.3.7.7.2. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
6.3.7.7.3. Atribuição de endereço IP nos clientes remotos de VPN SSL;
6.3.7.7.4. Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL;
6.3.7.7.5. Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD/LDAP e grupo de usuário AD/LDAP;
6.3.7.7.6. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
6.3.7.7.7. Atribuição de DNS nos clientes remotos de VPN;
6.3.7.7.8. Deve permitir que seja definido métodos de autenticação distintos por sistema operacional do dispositivo remoto de VPN (Android, IOS, Mac, Windows e Chrome OS);
6.3.7.7.9. A solução de VPN deve verificar se o client que está conectando é o mesmo para o qual o certificado foi emitido inicialmente. O acesso deve ser bloqueado caso o dispositivo não seja o correto;
6.3.7.7.10. Deve possuir lista de bloqueio para dispositivos que forem reportados com roubado ou perdido pelo usuário;
6.3.7.7.11. Deve haver a opção de ocultar o agente de VPN instalado no cliente remoto, tornando o mesmo invisível para o usuário;
6.3.7.7.12. Deve exibir mensagens de notificação customizada toda vez que um usuário remoto se conectar a VPN. Deve permitir que o usuário desabilite a exibição da mensagem nas conexões seguintes;
6.3.7.7.13. Deve avisar ao usuário remoto de VPN quanto a proximidade da expiração de senha LDAP. Deve permitir também a customização da mensagem com informações relevantes para o usuário;
6.3.7.7.14. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
6.3.7.7.15. A VPN SSL deve suportar proxy arp e uso de interfaces PPPOE;
6.3.7.7.16. Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local;
6.3.7.7.17. Deve permitir a distribuição de certificado para o usuário de remoto através do portal de VPN de forma automatizada;
6.3.7.7.18. Deve possuir lista de bloqueio para dispositivos em casos quando, por exemplo, o usuário reportar que o dispositivo foi perdido ou roubado;

6.3.7.7.19. Permite estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon;
6.3.7.7.20. Suporta leitura e verificação de CRL (certificate revocation list);
6.3.7.7.21. Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
6.3.7.7.22. O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN;
6.3.7.7.23. O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário,
6.3.7.7.24. Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:
6.3.7.7.24.1. Antes do usuário autenticar na estação;
6.3.7.7.24.2. Após autenticação do usuário na estação;
6.3.7.7.24.3. Sob demanda do usuário;
6.3.7.7.25. Deve Manter uma conexão segura com o portal durante a sessão.
6.3.7.7.26. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows 10, Windows 11, Mac OSx e Chrome OS;
6.3.7.7.27. O cliente de VPN SSL cliente-to-site também deve suportar dispositivos móveis (IOS e ANDROID) e sistemas operacionais Linux;
6.3.7.7.28. Deve possuir mecanismos de checagem de conformidade do dispositivo remoto;
6.3.7.7.29. A checagem de conformidade deve permitir verificar, no mínimo, as seguintes informações no cliente remoto: sistema operacional e patches instalados, antivírus e versão instalada, firewall no host, criptografia do disco, agente de DLP instalado, backup de disco, chaves de registros e processos ativos;
6.3.7.7.30. Deve ser possível a criação de perfis customizados de conformidade com, no mínimo, as seguintes opções: sistema operacional e patches instalados, antivírus e versão instalada, firewall no host, criptografia do disco, agente de DLP instalado backup de disco, chaves de registros e processos ativos;
6.3.7.7.31. O portal de VPN deve enviar ao cliente remoto, a lista de gateways de VPN ativos para estabelecimento da conexão, os quais devem poder ser administrados centralmente;
6.3.7.7.32. Deve haver a opção do cliente remoto escolher manualmente o gateway de VPN e de forma automática através da melhor rota entre os gateways disponíveis com base no tempo de resposta mais rápido;
6.3.7.7.33. Deve possuir a capacidade de identificar se a origem da conexão de VPN é externa ou interna;

6.3.8. Subscrição de Licença de Gerência Centralizada com suporte para 100 dispositivos Palo Alto Networks

6.3.8.1. O gerenciamento centralizado poderá ser entregue como appliance físico ou virtual. Caso seja entregue em appliance físico deve ser compatível com rack 19 polegadas e possuir todos os acessórios necessários para sua instalação. Caso seja entregue em appliance virtual deve ser compatível com Nutanix AHV;
6.3.8.2. A solução devera gerencia o quantidade total de equipamentos de ambos os lotes;
6.3.8.3. Caso a solução possua licenciamento relacionado ao volume de logs diários, este deve ser entregue com a maior capacidade suportada ou ilimitada sem a necessidade de licenciamento adicional;
6.3.8.4. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança.
6.3.8.5. Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções.
6.3.8.6. Deve permitir controle global de políticas para todos os equipamentos que compõe a plataforma de segurança;
6.3.8.7. Deve suportar organizar os dispositivos administrados em grupos: os sistemas virtuais devem ser administrados como dispositivos individuais, os grupos podem ser geográficos, por funcionalidade (por exemplo, IPS), e distribuição;
6.3.8.8. Deve implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular em grupos de firewalls;
6.3.8.9. Deve implementar a criação de perfis de usuários com acesso a plataforma de gerenciamento com definição exata de quais informações e de quais firewalls e grupos de firewalls o usuário terá acesso referente a logs e relatórios;
6.3.8.10. Deve permitir a criação de objetos e políticas compartilhadas;
6.3.8.11. Deve consolidar logs e relatórios de todos os dispositivos administrados;
6.3.8.12. Deve permitir que exportar backup de configuração automaticamente via agendamento;
6.3.8.13. Deve permitir que a configuração dos firewalls seja importada de forma automática na plataforma de gerenciamento centralizado e que possa ser usada em outros firewalls e grupos de firewalls;
6.3.8.14. Deve mostrar os status dos firewalls em alta disponibilidade a partir da plataforma de gerenciamento centralizado;

6.3.8.15. Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;
6.3.8.16. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
6.3.8.17. Deve permitir substituir o certificado de fábrica no acesso HTTPS a gerência do firewall como possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa;
6.3.8.18. Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows e Linux;
6.3.8.19. O gerenciamento deve permitir/possuir:
6.3.8.19.1. Criação e administração de políticas de firewall e controle de aplicação;
6.3.8.19.2. Criação e administração de políticas de IPS, Antivírus e Anti-Spyware;
6.3.8.19.3. Criação e administração de políticas de Filtro de URL;
6.3.8.19.4. Monitoração de logs;
6.3.8.19.5. Ferramentas de investigação de logs;
6.3.8.19.6. Debugging;
6.3.8.19.7. Captura de pacotes;
6.3.8.19.8. Acesso concorrente de administradores.
6.3.8.20. Deve permitir que administradores concorrentes façam modificações, valide configurações e reverta configurações do firewall simultaneamente e que cada administrador consiga aplicar apenas as suas alterações de forma independente das realizadas por outro administrador;
6.3.8.21. Deve possuir mecanismo busca global na solução onde possa se consultar por uma string tais como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso dos mesmo na configuração do dispositivo;
6.3.8.22. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;
6.3.8.23. Deve permitir usar palavras-chaves e cores para facilitar identificação de regras;
6.3.8.24. Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;
6.3.8.25. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
6.3.8.26. Autenticação integrada ao Microsoft Active Directory e servidor Radius;
6.3.8.27. Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;
6.3.8.28. Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;
6.3.8.29. Criação de regras que fiquem ativas em horário definido;
6.3.8.30. Criação de regras com data de expiração;
6.3.8.31. Backup das configurações e rollback de configuração para a última configuração salva;
6.3.8.32. Suportar Rollback de Sistema Operacional para a última versão local;
6.3.8.33. Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;
6.3.8.34. Deve possuir mecanismo de análise de impacto na política de segurança antes de atualizar a base com novas aplicações disponibilizadas pelo fabricante e validação de regras antes da aplicação;
6.3.8.35. Deve implementar mecanismo de validação de configurações antes da aplicação das mesmas permitindo identificar erros, tais como: rota de destino inválida, regras em shadowing etc;
6.3.8.36. É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação.
6.3.8.37. Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
6.3.8.38. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
6.3.8.39. Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;
6.3.8.40. Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;
6.3.8.41. Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;
6.3.8.42. Deve permitir a criação de Dashboards customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, antivírus, Anti-Spyware, malwares "Zero Day"detectados em sand-box e tráfego bloqueado;
6.3.8.43. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;
6.3.8.44. Dever permitir a visualização dos logs de malwares modernos, tráfego (IP de origem, destino, usuário e porta), aplicação, IPS, antivírus, Anti-Spyware, Filtro de URL e filtro de arquivos em uma única tela.
6.3.8.45. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Spware), etc;

6.3.8.46. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e Anti-Spware), e URLs que passaram pela solução;
6.3.8.47. Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em Real Time;
6.3.8.48. Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso;
6.3.8.49. Deve possuir relatório de visibilidade e uso sobre aplicativos (SaaS). O relatório também deve mostrar 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;
6.3.8.50. Os relatórios de visibilidade e uso sobre aplicativos (SaaS) devem poder ser extraídos por grupo de usuários apresentando o uso e consumo de aplicações por grupo de usuário;
6.3.8.51. Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado;
6.3.8.52. Deve permitir fazer o envio de logs para soluções externas de forma granular podendo selecionar quais campos dos logs serão enviados incluindo, mas não limitado a: tipo de ameaça, usuário, aplicação, etc;
6.3.8.53. Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):
6.3.8.53.1. Situação do dispositivo e do cluster;
6.3.8.53.2. Principais aplicações;
6.3.8.53.3. Principais aplicações por risco;
6.3.8.53.4. Administradores autenticados na gerência da plataforma de segurança;
6.3.8.53.5. Número de sessões simultâneas;
6.3.8.53.6. Status das interfaces;
6.3.8.53.7. Uso de CPU.
6.3.8.54. Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:
6.3.8.54.1. Resumo gráfico de aplicações utilizadas;
6.3.8.54.2. Principais aplicações por utilização de largura de banda de entrada e saída;
6.3.8.54.3. Principais aplicações por taxa de transferência de bytes;
6.3.8.54.4. Principais hosts por número de ameaças identificadas;
6.3.8.54.5. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Spware), de rede vinculadas a este tráfego.
6.3.8.55. Deve permitir a criação de relatórios personalizados;
6.3.8.56. Gerar alertas automáticos via:
6.3.8.56.1. Email;
6.3.8.56.2. SNMP;
6.3.8.56.3. Syslog;
6.3.9. Serviço de instalação das soluções de Next-Generation Firewall Palo Alto Networks

6.3.9.1. O Serviço de instalação das unidades deverá ser realizado da seguinte forma:
6.3.9.1.1. Para a renovação, deverá ser realizado ativação das novas licenças e atualização de versão dos appliances.
6.3.9.1.2. Os serviços de instalação dos firewalls PA-410 serão feitos de forma remota pela CONTRATADA.
6.3.9.1.3. Os serviços de instalação dos firewalls PA-5410 serão feitos de forma presencial na unidade definida pelo TJAM;
6.3.9.1.4. Todo o processo será realizado por profissional qualificado e certificado na solução.
6.3.9.1.5. Os serviços de instalação e configuração das soluções serão supervisionados pela contratante, através de funcionário (os) designado (s) para esta atividade, preliminarmente ao início da execução, durante a execução até o término da execução da instalação e ser acompanhada por gerente de projetos da CONTRATADA visando atender os prazos definidos e suas entrega de todo lote.
6.3.9.1.6. A instalação e configuração das soluções deverá ser realizada pela equipe da própria CONTRATADA.
6.3.9.1.7. A instalação e configuração da solução não poderá ocorrer por empresa, equipe ou profissional diferente da CONTRATADA neste processo.
6.3.9.1.8. A instalação e configuração contempla toda parte de hardware e software conforme item e arquitetura da solução Segurança para Defesa Cibernética.
6.3.9.1.9. Entende-se como instalação e configuração a instalação dos softwares e a ativação dos equipamentos adquiridos pela contratante.
6.3.9.1.10. A CONTRATADA executará os serviços sem qualquer interferência no funcionamento regular das atividades normalmente realizadas pela contratante, garantindo a continuidade dos serviços, ou seja, não poderá haver interrupção não programada do serviço de dados atual para a entrada do novo serviço. Desta forma, executará serviços em finais de semana, feriados e horário noturno, sempre que houver necessidade para atendimento das condições expostas pela contratante nesta especificação;
6.3.9.1.11. Todas as instalações e configurações serão realizadas em conformidade com a recomendação do fabricante do equipamento e os requisitos fornecidos pela contratante para o ambiente em questão;
6.3.9.1.12. Instalação logica em ambiente virtual da contratante;

6.3.9.1.13. Ao término da instalação e configuração poderá ser considerado uma sessão de perguntas e respostas no local, com o objetivo de ser abordado os pontos principais e de funcionalidades chaves dos produtos instalados.
6.3.9.1.14. A CONTRATADA deverá seguir sua metodologia própria no processo de instalação e as melhores práticas indicadas pelo fabricante.
6.3.9.1.15. A CONTRATADA deverá responsabilizar-se pela conformidade e qualidade dos serviços e bens, bem como de cada material, matéria-prima ou componente individualmente considerado, mesmo que não sejam de sua fabricação, garantindo seu perfeito desempenho;

6.3.10. Garantia da Solução de Plataforma de Segurança Palo Alto Networks, com suporte Premium oficial 24x7:

6.3.10.1. A CONTRATADA deverá disponibilizar uma equipe de pessoas tecnicamente capacitadas, as quais serão responsáveis pelo suporte e manutenção das soluções durante todo o contrato de forma remota.
6.3.10.2. A equipe deverá estar disponível para atendimento em regime 24 horas, 7 dias na semana e 365 dias ao ano.
6.3.10.3. Responsabilidades e atividades da Equipe:
6.3.10.3.1. Realizar todos os serviços de suporte e manutenção da solução quando solicitado pela CONTRATANTE.
6.3.10.3.2. Realizar o atendimento de tickets/chamados abertos pela contratante no sistema da CONTRATADA quando solicitado pela CONTRATANTE.
6.3.10.3.3. Realizar a interface entre as necessidades da contratante e os profissionais do fabricante por executar as atividades, em caso de necessidade de intervenção do fabricante em soluções de problemas.
6.3.10.4. A CONTRATADA deverá disponibilizar ferramenta de acompanhamento de chamados, de sua propriedade e de sua responsabilidade, que atendam aos seguintes requisitos:
6.3.10.4.1. O acesso às informações deverá ser protegido por senha e conexão segura ou outro método equivalente;
6.3.10.4.2. A contratante deverá ter acesso à ferramenta via interface WEB através da internet;
6.3.10.4.3. A ferramenta deverá manter identificação do projeto ou demanda, data e hora de abertura do chamado, início e término do atendimento, identificação e resolução do escopo, documentação da solução, status, recursos alocados e outras informações pertinentes;
6.3.10.4.4. A ferramenta deverá ser capaz de exportar seus dados em formato .csv;
6.3.10.5. A ferramenta deverá ser capaz de permitir a emissão de relatórios diários e/ou mensais para o controle de todas as solicitações abertas e encaminhadas pela contratante;
6.3.10.5.1. A ferramenta deverá ser capaz de gerir e garantir que os níveis de serviços de atendimento sejam monitorados, de forma que o tempo de atendimento de uma solicitação comece a ser contado a partir do envio da mesma pelo usuário solicitante e seja finalizado no momento de fechamento da solicitação no sistema.

6.3.11. Firewall Palo Alto PA-5410

6.3.11.1. Deve possuir throughput de, no mínimo, 40 (quarenta) Gbps com a funcionalidade de controle de aplicação para todas as assinaturas que o fabricante possuir;
6.3.11.2. Deve possuir throughput de, no mínimo, 20 (vinte) Gbps com as funcionalidades de controle de aplicação, IPS, Antivírus e Anti-Spyware habilitadas simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os throughput aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real;
6.3.11.3. Deve suportar, no mínimo, 3.000(três milhões) conexões simultâneas;
6.3.11.4. Deve suportar, no mínimo, 250.000 (duzentos e cinquenta mil) novas conexões por segundo;
6.3.11.5. Deve possuir, no mínimo, 6 (seis) interfaces físicas de rede de 1Gbps do tipo RJ-45;
6.3.11.6. Deve possuir, no mínimo, 6 (seis) interfaces físicas de rede de 10Gbps SFP/SFP+;
6.3.11.7. Deve possuir, no mínimo, 4 (quatro) interfaces físicas de rede de 10/25Gbps SFP/SFP+/SFP28;
6.3.11.8. Deve possuir, no mínimo, 4 (quatro) interfaces físicas de rede de 40/100Gbps QSFP+/QSFP28;
6.3.11.9. Deve possuir, no mínimo, 1 (uma) interface física de rede de 1 Gbps dedicada para gerenciamento out of band, ou seja, não será permitida a utilização de interfaces genéricas e não dedicadas para o fim;
6.3.11.10. Deve possuir, no mínimo, 1 (uma) interface física do tipo console ou similar;
6.3.11.11. Deve estar licenciada para no mínimo 10 sistemas virtuais;
6.3.11.12. Deve possuir armazenamento interno de, no mínimo, 480 (quatrocentos e oitenta) GB para registro de logs;
6.3.11.13. Deve possuir fonte de alimentação elétrica redundante capaz de operar entre 120 a 240 VAC;

6.4. Controle de Aplicações

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

6.4.3. Reconhecer pelo menos 3000 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
6.4.4. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443.
6.4.5. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
6.4.6. Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo, mas não limitado a Skype. Deve permitir também a criação de políticas de exceção concedendo o acesso a aplicativos como Skype apenas para alguns usuários;
6.4.7. Identificar o uso de táticas evasivas via comunicações criptografadas;
6.4.8. Atualizar a base de assinaturas de aplicações automaticamente;
6.4.9. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;
6.4.10. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
6.4.11. Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
6.4.12. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística;
6.4.13. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
6.4.14. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;
6.4.15. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
6.4.16. Deve alertar o usuário quando uma aplicação for bloqueada;
6.4.17. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;
6.4.18. Deve permitir criar filtro na tabela de regras de segurança para exibir somente:
6.4.19. Regras que permitem passagem de tráfego baseado na porta e não por aplicação, exibindo quais aplicações estão trafegando na mesma, o volume em bytes trafegado por cada a aplicação por, pelo menos, os últimos 30 dias e o primeiro e último registro de log de cada aplicação trafegada por esta determinada regra;
6.4.20. Aplicações permitidas em regras de forma desnecessária, pois não há tráfego da mesma na determinada regra;
6.4.21. Regras de segurança onde não houve passagem de tráfego nos últimos 90 dias;

6.5. Identificação de Usuários

6.5.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-Directory e base de dados local;
6.5.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
6.5.3. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
6.5.4. Deve possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
6.5.5. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via syslog, para a identificação de endereços IP e usuários;
6.5.6. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
6.5.7. Suporte a autenticação Kerberos;
6.5.8. Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, captive Portal e usuário de VPN SSL;
6.5.9. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
6.5.10. O firewall deve operar/suportar Security Assertion Markup Language (SAML) 2.0, com single sign-on para as funcionalidades de Captive Portal e VPN SSL (client to server), permitindo login único e interativo para fornecer acesso automático a serviços autenticados, internos e externos à organização;

6.5.11. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

6.6. QoS:

6.6.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, 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 máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.
6.6.2. Suportar a criação de políticas de QoS por:
6.6.3. Endereço de origem
6.6.4. Endereço de destino
6.6.5. Por usuário e grupo do LDAP/AD.
6.6.6. Por aplicações;
6.6.7. Por porta;
6.6.8. O QoS deve possibilitar a definição de classes por:
6.6.9. Banda Garantida
6.6.10. Banda Máxima
6.6.11. Fila de Prioridade.
6.6.12. Suportar priorização Real Time de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.
6.6.13. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
6.6.14. Deve implementar QOS (traffic-shapping), para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (inbound e outbound);
6.6.15. Disponibilizar estatísticas Real Time para classes de QoS.
6.6.16. Deve suportar QOS (traffic-shapping), em interface agregadas;
6.6.17. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

6.7. Acordo de Nível de Serviço.

6.7.1. O tempo de início ao atendimento às ocorrências deverá ocorrer de acordo com o nível de severidade definido na abertura do chamado;

6.7.2. Os prazos estabelecidos nos níveis de serviços serão contados a partir da abertura do chamado e será classificado conforme as severidades especificadas a seguir:

6.7.2.1. **Alta:** significa que há um problema crítico, causando séria interrupção nos serviços do TJAM; isso inclui a indisponibilidade de 01 (um) ou mais recursos da solução contratada e (ou) a indisponibilidade de um dos equipamentos que compõe a solução. Nestes casos será estipulado o prazo máximo de 01 (uma) hora para atendimento e 04 (quatro) horas para completa restauração do ambiente e das funcionalidades da solução contratada. Com o prazo sendo contado a partir do momento de abertura do chamado.

6.7.2.2. **Média:** ocorre quando uma ou mais funcionalidades importantes da solução contratada são afetados por problemas persistentes que afetam muitos usuários mas não causa total interrupção nos serviços do TJAM. Nestes casos é estipulado o prazo máximo de 02 (duas) horas úteis para atendimento e 08 (oito) horas úteis para resolução ou solução alternativa, contados a partir do momento de abertura do chamado.

6.7.2.3. **Baixa:** nesta categoria serão agrupados os chamados onde o cliente solicita informações, consultoria, atividades preventivas, mudanças programadas ou assistência sobre capacidades, instalação ou configuração de componentes, não havendo impacto e urgência. Neste caso a CONTRATADA tem um prazo de até 02 (dois) dias úteis para iniciar o atendimento e 05 (cinco) dias úteis para resolução ou solução alternativa, contados a partir do momento de abertura do chamado.

6.7.3. Para os chamados de qualquer severidade, a critério da CONTRATANTE, poderá ser agendado o melhor horário para atendimento, onde será contabilizado o tempo de resolução a partir do horário agendado;

6.7.4. O fechamento de qualquer chamado só poderá ocorrer mediante consulta prévia a CONTRATANTE quanto à efetiva solução do problema;

6.7.5. Qualquer chamado fechado, sem anuência da CONTRATANTE ou sem que o problema tenha sido resolvido, será reaberto e os prazos serão contados a partir da abertura original do chamado, inclusive para efeito de aplicação das sanções previstas;

6.7.6. A CONTRATADA manterá cadastro das pessoas indicadas pela CONTRATANTE que poderão efetuar abertura e autorizar o fechamento de chamados;

7. DA CARACTERIZAÇÃO DO OBJETO

7.1. Os itens do objeto **enquadram-se na categoria de bens e serviços comuns**, de que trata a Lei nº 10.520, de 17 de julho de 2002, por possuírem padrões de desempenho e características gerais e específicas usualmente encontradas no mercado.

8. QUANTITATIVO

8.1. Os itens que constituem o grupo de renovação das licenças de software da solução de Firewall Palo Alto estão compreendidos no intervalo que vai de 1 a 4.

8.2. Os itens que constituem o grupo de expansão da solução de firewall para o ambiente de datacenter e unidades descentralizadas estão compreendidos no intervalo que vai de 5 a 18.

Renovação e expansão de solução de firewall para o ambiente de datacenter e unidades descentralizadas			
ITEM	**ESPECIFICAÇÕES**	**QUANTIDADE MÍNIMA POR CONTRATAÇÃO**	**QUANTIDADE TOTAL**
1	Subscrição de Prevenção a Ameaças para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.	2	2
2	Subscrição de Filtro de URL para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.	2	2
3	Subscrição de Análise de Malware para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.	2	2
4	Garantia da Solução de Plataforma de Segurança Palo Alto Networks PA-5220, com suporte Premium oficial Palo Alto Networks 24x7 em Alta Disponibilidade, pelo período de 60 meses.	2	2
5	Firewall Palo Alto PA-410	10	70
6	Subscrição CORE SECURITY SUBSCRIPTION BUNDLE (ADVANCED THREAT PREVENTION, ADVANCED URL FILTERING, ADVANCED WILDFIRE, DNS SECURITY AND SD-WAN), pelo período de 60 meses.	10	70
7	Garantia da Solução de Plataforma de Segurança Palo Alto Networks PA-410, com suporte Premium oficial Palo Alto Networks 24x7, pelo período de 60 meses.	10	70
8	Subscrição de Licença de Gerência Centralizada com suporte para 100 dispositivos Palo Alto Networks, pelo período de 60 meses.	1	1
9	Garantia da Solução de Panorama, com suporte Premium oficial Palo Alto Networks 24x7, pelo período de 60 meses.	1	1
10	Subscrição de DNS Seguro para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.	2	2
11	Subscrição de SD-WAN Seguro para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.	2	2
12	Serviço de instalação das soluções de Next-Generation Firewall Palo Alto Networks PA-410 e PA-5410.	12	72
13	Treinamento oficial do fabricante remoto, em língua portuguesa, com disponibilização de voucher para certificação de administração da solução Palo Alto.	2	4
14	Subscrição de GlobalProtect para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.	2	2
15	Firewall Palo Alto PA-5410	2	2
16	Subscrição CORE SECURITY SUBSCRIPTION BUNDLE (ADVANCED THREAT PREVENTION, ADVANCED URL FILTERING, ADVANCED WILDFIRE, DNS SECURITY AND SD-WAN) para PA-5410, pelo período de 60 meses.	2	2
17	Garantia da Solução de Plataforma de Segurança Palo Alto Networks PA-5410, com suporte Premium oficial Palo Alto Networks 24x7, pelo período de 60 meses.	2	2

18	Subscrição de GlobalProtect para solução de Plataforma de Segurança Palo Alto Networks PA-5410, pelo período de 60 meses.	2	2

8.3. Da estimativa de quantidades a serem adquiridas pelo órgão gerenciador e órgãos participantes.

8.3.1. O quantitativo total registrado deverá ser utilizado pelo órgão gerenciador e órgãos participantes, se houver, de maneira remanejada, de tal forma que o total aderido (gestor + participantes) não ultrapasse o quantitativo total registrado.

8.4. Da estimativa de quantidades a serem adquiridas por órgãos não participantes.

8.4.1 Por não gerar elevado custo administrativo a este Tribunal de Justiça, bem como por ser um procedimento comum e corriqueiro, será possível a adesão de órgãos não Participantes, inclusive órgãos e entidade do Poder Executivo Estadual, mediante anuência do órgão Gerenciador, conforme regramentos do Decreto n. 40.674/2019;
8.4.2 Os órgãos e entidade que não participaram do registro de preços, quando desejarem fazer uso da ata de registro de preços, deverão consultar o Órgão Gerenciador da ata para manifestação sobre a possibilidade de adesão;
8.4.3 Caberá ao fornecedor beneficiário da ata de registro de preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento decorrente de adesão, desde que não prejudique as obrigações presentes e futuras decorrentes da ata, assumidas com o Órgão Gerenciador e Órgãos Participantes;
8.4.4 As aquisições ou contratações adicionais a que se refere este artigo, observarão os seguintes limites:
8.4.4.1 O quantitativo, por órgão ou entidade, não poderá exceder a 50% (cinquenta por cento) do quantitativo do item registrado na ata de registro de preços; e
8.4.4.2 O somatório das adesões não poderá ultrapassar o limite de 2 (duas) vezes o quantitativo de cada item registrado na ata de registro de preços;
8.4.5 Compete ao Órgão não Participante os atos relativos à cobrança do cumprimento pelo fornecedor das obrigações contratualmente assumidas e a aplicação, observada ampla defesa e o contraditório, de eventuais penalidades decorrentes do descumprimento de cláusulas contratuais, em relação às suas próprias contratações oriundas do registro de preços, informando as ocorrências ao Órgão Gerenciador;
8.4.6 É facultada aos órgãos e entidades do Poder Executivo do Estado do Amazonas a adesão à ata de registro de preços promovida por outros Estados e pela União (Decreto n. 40.674/2019).

9. FORMA DE FORNECIMENTO

9.1. O objeto da contratação possui características comuns e usuais, fornecido por várias empresas, porém deverá ser realizada por único fornecedor. O parcelamento do objeto, neste caso, é inviável já que não se justifica técnica e economicamente, além do que a solução de TI contratada é composta de serviços integrados e correlatos que visam manter em funcionamento toda infraestrutura de solução;

9.2. Portanto, o fornecimento do objeto será no regime de empreitada por preço global.

10. CRONOGRAMA DE EXECUÇÃO

10.1. Não se faz necessário estabelecer cronograma de execução dos serviços de renovação do licenciamento de software da solução de Firewall de Datacenter.

10.2. O cronograma de execução dos serviços de expansão da solução de firewall para o ambiente de datacenter e unidades descentralizadas será definido juntamente com a CONTRATADA após assinatura do contrato.

11. DA SOLICITAÇÃO DOS SERVIÇOS

11.1. A CONTRATADA deverá disponibilizar central de atendimento para a abertura e fechamento de chamados técnicos, conforme o Acordo de Nível de Serviço estabelecido neste TR.

11.2. No início da vigência do contrato, a CONTRATADA deverá indicar os canais para solicitação e acompanhamento dos serviços.

12. VALOR ESTIMADO DA CONTRATAÇÃO

12.1. A estimativa de custo dos itens a serem adquiridos ou prestados, constantes deste Termo de Referência, será discriminada nas planilhas

de valor estimado, de competência da Secretaria de Compras, Contratos e Operações (SECOP), conforme o quadro abaixo:

ITEM	QUANTIDADE	ESPECIFICAÇÕES	VALOR ESTIMADO	
			UNITÁRIO	TOTAL
1	2	Subscrição de Prevenção a Ameaças para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.		
2	2	Subscrição de Filtro de URL para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.		
3	2	Subscrição de Análise de Malware para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.		
4	2	Garantia da Solução de Plataforma de Segurança Palo Alto Networks PA-5220, com suporte Premium oficial Palo Alto Networks 24x7 em Alta Disponibilidade, pelo período de 60 meses.		
5	70	Firewall Palo Alto PA-410		
6	70	Subscrição CORE SECURITY SUBSCRIPTION BUNDLE (ADVANCED THREAT PREVENTION, ADVANCED URL FILTERING, ADVANCED WILDFIRE, DNS SECURITY AND SD-WAN), pelo período de 60 meses.		
7	70	Garantia da Solução de Plataforma de Segurança Palo Alto Networks PA-410, com suporte Premium oficial Palo Alto Networks 24x7, pelo período de 60 meses.		
8	1	Subscrição de Licença de Gerência Centralizada com suporte para 100 dispositivos Palo Alto Networks, pelo período de 60 meses.		
9	1	Garantia da Solução de Panorama, com suporte Premium oficial Palo Alto Networks 24x7, pelo período de 60 meses.		
10	2	Subscrição de DNS Seguro para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.		
11	2	Subscrição de SD-WAN Seguro para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.		
12	72	Serviço de instalação das soluções de Next-Generation Firewall Palo Alto Networks PA-410 e PA-5410.		
13	4	Treinamento oficial do fabricante remoto, em língua portuguesa, com disponibilização de voucher para certificação de administração da solução Palo Alto.		
14	2	Subscrição de GlobalProtect para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.		
15	2	Firewall Palo Alto PA-5410		
16	2	Subscrição CORE SECURITY SUBSCRIPTION BUNDLE (ADVANCED THREAT PREVENTION, ADVANCED URL FILTERING, ADVANCED WILDFIRE, DNS SECURITY AND SD-WAN) para PA-5410, pelo período de 60 meses.		
17	2	Garantia da Solução de Plataforma de Segurança Palo Alto Networks PA-5410, com suporte Premium oficial Palo Alto Networks 24x7, pelo período de 60 meses.		
18	2	Subscrição de GlobalProtect para solução de Plataforma de Segurança Palo Alto Networks PA-5410, pelo período de 60 meses.		
			TOTAL	

12.2. O critério de julgamento para escolha da melhor proposta será o de menor preço global.

13. DA NECESSIDADE DE CONTRATO

13.1. A adesão à Ata de Registro de Preços (ARP) procedente deste certame resultará em formalização de contrato para os serviços previstos neste termo de referência, tendo em vista as características do objeto a ser contratado, com a existência de obrigações futuras, incluindo a garantia, continuidade e confiabilidade do mesmo nos termos do art. 62 da Lei 8.666/93.

13.2. Considerando que todos os itens da ARP serão pagos em parcela única após a entrega do equipamento, ativação ou realização do serviço, os preços contratuais não poderão ser reajustados.

14. PERÍODO DE VIGÊNCIA E REPACTUAÇÃO

14.1 O contrato, nos termos do art. 57, inc. II da Lei 8.666/93, deverá ter período de vigência de 60 (sessenta) meses a contar da data da assinatura do mesmo.

15. OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATANTE

15.1. Orientar a execução do objeto;
15.2. Fornecer, em tempo hábil, todos os dados técnicos e informações de sua responsabilidade, necessários ao fornecimento do objeto;
15.3. Efetuar os pagamentos, no prazo e nas condições indicados no contrato, relativamente ao fornecimento do objeto, comunicando à CONTRATADA quaisquer irregularidades ou problemas que possam inviabilizar os pagamentos.
15.4. Receber os itens objetos deste fornecimento, emitindo Atestado de Recebimento na Nota Fiscal/Fatura.
15.5. Designar responsáveis para o acompanhamento e fiscalização da boa execução do contrato e aplicar as medidas corretivas necessárias, inclusive as penalidades contratual e legalmente previstas, comunicando à CONTRATADA as ocorrências que, a seu critério, exijam medidas corretivas.
15.6. Solicitar o reparo, a correção, a remoção, a reconstrução ou a substituição do objeto do contrato, nos casos em que se verificarem vícios, defeitos ou incorreções.
15.7. Comunicar formalmente qualquer anormalidade ocorrida na execução do objeto adquirido
15.8. Proporcionar todas as facilidades indispensáveis à boa execução das obrigações contratuais, inclusive permitindo o acesso de empregados, prepostos ou representantes da CONTRATADA às dependências do Tribunal;
15.9. Prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos da CONTRATADA

16. OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA

16.1. Fornecer, sob sua integral responsabilidade, os itens objetos deste TR, devendo receber prévia aprovação do TJAM, que se reserva o direito de rejeitá-los.
16.2. Correrá por conta do CONTRATADO todas as despesas concernentes ao fornecimento do objeto licitado, dentre as quais os encargos trabalhistas, previdenciários, fiscais e comerciais.
16.3. Ressarcir os eventuais prejuízos causados ao CONTRATADO ou a terceiros, provocados por ineficiência ou irregularidades cometidas na execução das obrigações assumidas por força do contrato.
16.4. Segurança Institucional
16.4.1. A CONTRATADA não poderá divulgar, mesmo em caráter estatístico, quaisquer informações originadas no TJAM sem prévia autorização formal;
16.4.2. A CONTRATADA será expressamente responsabilizada quanto à manutenção de sigilo sobre quaisquer dados, informações, artefatos, contidos em quaisquer documentos e em quaisquer mídias, de que venha a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto divulgar, reproduzir ou utilizar, independentemente da classificação de sigilo conferida pelo contratante a tais documentos.
16.5. Deveres e responsabilidades da CONTRATADA
16.5.1. Envidar todo o empenho necessário ao fiel e adequado cumprimento dos encargos que lhe são confiados;
16.5.2. Apresentar, na data da assinatura do contrato, declaração assinada pelo representante legal da empresa indicando preposto para representá-la durante a execução;
16.5.3. Prestar a garantia e suporte técnico de hardware e software, objeto da contratação, a partir da assinatura do termo de recebimento definitivo
16.5.4. Fornecer peças, serviços e materiais necessários e indispensáveis à boa execução dos serviços;
16.5.5. Fornecer mão de obra qualificada e suficiente para execução das tarefas pertinentes ao serviço contratado;
16.5.6. Fornecer, em caso de substituição de equipamentos, peças, componentes e outros materiais necessários, sempre novos, homologados pelo fabricante do equipamento e possuir características iguais ou superiores ao item substituído, devendo sempre passar pela avaliação da equipe técnica do TJAM;
16.5.7. Responder pelas despesas relativas a encargos trabalhistas, seguro de acidentes, impostos, contribuições previdenciárias e quaisquer outras que forem devidas e referentes aos serviços executados por seus empregados, uma vez inexistir, no caso, vínculo empregatício deles com a Contratante;
16.5.8. Manter, durante toda a execução contrato, todas as condições de habilitação exigidas para a contratação;
16.5.9. Não transferir a terceiros, por qualquer forma, nem mesmo parcialmente, as obrigações assumidas, nem subcontratar qualquer das prestações a que está obrigada;
16.5.10. Disponibilizar central de atendimento para a abertura e fechamento de chamados técnicos, conforme períodos, horários e condições estabelecidas neste TR;
16.5.11. Comunicar formal e imediatamente ao Gestor ou Responsável Técnico do TJAM sobre mudanças nos dados para contato com a central de atendimento;

16.5.12. Prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos do TJAM, referentes a qualquer problema detectado ou ao andamento de atividades da garantia;
16.5.13. Respeitar as normas e procedimentos de controle e acesso às dependências do TJAM;
16.5.14. Manter, ainda, os seus funcionários e prepostos identificados por crachá, quando em trabalho, devendo substituir imediatamente qualquer um deles que seja considerado inconveniente à boa ordem e às normas disciplinares do TJAM;
16.5.15. Cumprir e garantir que seus profissionais estejam cientes, aderentes e obedeçam rigorosamente às normas e aos procedimentos estabelecidos na Política de Segurança da Informação do TJAM;
16.5.16. Responder pelos danos causados diretamente à administração do TJAM ou a terceiros, decorrentes de sua culpa ou dolo, durante o fornecimento e a execução dos serviços, não excluindo ou reduzindo essa responsabilidade à fiscalização ou o acompanhamento pelo TJAM, procedendo imediatamente aos reparos ou às indenizações cabíveis e assumindo o ônus decorrente;
16.5.17. Responder, ainda, por quaisquer danos causados diretamente aos equipamentos ou a outros bens de propriedade do TJAM, quando esses tenham sido ocasionados por seus funcionários durante o fornecimento e a prestação dos serviços, procedendo imediatamente aos reparos ou às indenizações cabíveis e assumindo o ônus decorrente;
16.5.18. Arcar com despesa decorrente de qualquer infração seja qual for, desde que praticada por seus funcionários no recinto do TJAM ou através de acesso remoto;
16.5.19. Comunicar ao TJAM qualquer anormalidade de caráter urgente e prestar os esclarecimentos julgados necessários;
16.5.20. Manter em compatibilidade com as obrigações a serem assumidas, durante toda a execução do contrato, todas as condições de habilitação e de qualificação na licitação;
16.5.21. Cumprir com os prazos estipulados no Termo de Referência / Edital;
16.5.22. Autorizar e assegurar o TJAM o direito de fiscalizar, sustar e/ou recusar os produtos que não estejam de acordo com as especificações constantes da Proposta da CONTRATADA;
16.5.23. Manter sigilo sobre todo e qualquer assunto de interesse do TJAM ou de terceiros de que tomar conhecimento em razão da execução do objeto, respeitando todos os critérios estabelecidos, aplicáveis aos dados, informações, regras de negócios, documentos, entre outros pertinentes, sob pena de responsabilidade civil, penal e administrativa;
16.5.24. Todas as taxas e impostos que incidam ou venham a incidir sobre este contrato ou sobre os serviços a ele vinculados correrão por conta da CONTRATADA.

17. DA SUBCONTRATAÇÃO DE SERVIÇOS
17.1. Não será permitida a subcontratação do objeto desta licitação, ficando sob a inteira responsabilidade do licitante contratado o cumprimento de todas as condições contratuais, atendendo aos requisitos técnicos e legais para esta finalidade.

18. DA GARANTIA OU ASSISTÊNCIA TÉCNICA
18.1. Nos termo do art. 56 da Lei 8.666/93, a contratada deverá optar por uma das modalidades de garantia, em conformidade com §2º art. 56. da Lei 8.666/93, podendo ser renovada a cada prorrogação, ressalvado o previsto no parágrafo 3º do supracitado artigo.

19. DA QUALIFICAÇÃO TÉCNICA
19.1. Atestado(s) de Capacidade Técnica, em nome da licitante, expedido(s) por Pessoa Jurídica de direito público ou privado, que comprove(m) que a licitante (Pessoa Jurídica) forneceu:
19.1.1. Atestado(s) de capacidade técnica que comprove fornecimento e suporte de solução de Next-Generation Firewall por no mínimo 12 meses.
19.1.2. Atestado(s) de capacidade técnica que comprove fornecimento e suporte de solução de conectividade SD-WAN por no mínimo 12 meses.
19.2. Será aceito somatória de atestados de capacidade técnica para comprovar a prestação dos serviços e fornecimento de soluções solicitados para comprovação.
19.2.1. Mediante solicitação da CONTRATANTE, a licitante deverá informar os dados de contato do(s) emitente(s) do(s) Atestado(s) (telefone, endereço, e-mail).
19.2.2. Caso o TJAM entenda necessário, poderão ser solicitadas as cópias dos contratos e aditivos da prestação do respectivo serviços e fornecimentos e das Notas Fiscais correspondentes aos Atestados apresentados, visto que poderão ser objeto de diligências para a verificação da autenticidade de seu conteúdo.
19.2.3. No caso de Atestados emitidos por empresa da iniciativa privada, não serão considerados aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa proponente. Serão considerados como pertencentes ao mesmo grupo empresarial da empresa proponente, empresas controladas ou controladoras da empresa proponente, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da empresa proponente.
19.2.4. Atestados emitidos por empresas do mesmo grupo empresarial contemplando os mesmos objetos no mesmo período serão considerados como um único Atestado, computando-se o de maior volume.
19.2.5. Conforme previsto no §3º do art. 43 da Lei nº 8.666/93, os Atestados de Capacidade Técnica apresentados poderão ser objeto de diligência a critério do CONTRATANTE, para verificação de

autenticidade de seu conteúdo. A impossibilidade de verificação tornará o Atestado inválido.
19.2.6. Encontrada divergência entre o especificado nos Atestados e o apurado em eventual diligência, inclusive validação do contrato de prestação de serviços entre o emissor do Atestado e a licitante, além da inabilitação no processo licitatório, fica sujeita a licitante às penalidades cabíveis.

20. VISTORIA TÉCNICA
20.1. O licitante poderá realizar vistoria nas instalações dos locais de execução dos serviços, acompanhado por servidor designado para esse fim, de segunda a sexta-feira das 08:00 às 14:00 horas, no horário local, devendo o agendamento ser efetuado de acordo com a unidade a ser visitada, conforme quadro abaixo:

Unidade	Setor	Contato para Agendamento
Tribunal Arnoldo Péres	Divisão de Infraestrutura de TIC	(92) 2129-6779

20.2. Os ANEXOS I e II possuem, respectivamente, o MODELO DO TERMO DE VISTORIA e o MODELO DE DECLARAÇÃO DE DISPENSA DE VISTORIA.

21. LOCAL OU PRAZO DE ENTREGA OU APLICAÇÃO
21.1. Os serviços serão prestados na Divisão de Infraestrutura de TIC (DVITIC) na Sede do TJAM e/ou remotamente.
21.2. Caberá ao TJAM efetuar a logística de movimentação e instalação física dos equipamentos adquiridos entre as unidades do TJAM na capital Manaus e no interior do Amazonas.
21.3. O prazo de entrega da solução NGFW PALO ALTO será de até, 10 (dez) dias corridos para as licenças de renovação e 90 (noventa) dias corridos para o fornecimento de hardware, a contar da assinatura do contrato.
21.4. A licitante vencedora deverá fazer a extensão das licenças dos equipamentos atuais até o recebimento definitivo dos novos appliances.
21.5. A solução NGFW PALO ALTO NETWORKS deverá ter seu registro junto ao fabricante para fins de garantia, atualização e suporte pelo período de 60 meses, em nome do TJAM.
21.6. Caso os produtos e/ou itens sejam diferentes da descrição contida neste Edital, ou apresentarem defeitos, serão considerados não entregues. A contagem do prazo de entrega não será interrompida em decorrência dos produtos rejeitados, arcando a licitante com o ônus decorrente deste atraso.
21.7. Os hardwares deverão ser entregue à Divisão de Patrimônio e Material, localizada no Subsolo do Fórum Ministro Henoch Reis, situado à Av. Humberto Calderaro Filho, s/n. Horário de 8:00 às 13:00 horas Tel.: (92) 3303 5233/5020.

22. DO RECEBIMENTO PROVISÓRIO E DEFINITIVO
22.1. O recebimento dos equipamentos será realizado em 2 (duas) etapas:
22.1.1. Provisoriamente, no momento da entrega dos equipamentos. Nesta etapa, o servidor ou a comissão designada procederá o recebimento dos equipamentos limitando-se a verificar o discriminado na Nota Fiscal e as especificações básicas, e fazendo constar no canhoto e no verso da Nota Fiscal a data da entrega, e se for o caso, as irregularidades observadas;
22.1.2. Definitivamente, no prazo de 10 (dez) dias, contados do recebimento provisório. Nessa etapa o servidor ou a comissão designada verificará as especificações dos equipamento entregues em face ao exigido no Termo de Referência e o ofertado na proposta de preço.
22.2. Os materiais poderão ser recusados se não atenderem às especificações dispostas no Termo de Referência e na proposta de preço.
22.3 Ocorrendo a hipótese prevista no item acima, a contratada deverá providenciar a substituição do equipamento no prazo máximo de 15 (quinze) dias, contados a partir da comunicação do Tribunal de Justiça do Estado do Amazonas acerca do não aceite.

23. DO PAGAMENTO
23.1. O pagamento será realizado em moeda corrente nacional, mediante Ordem Bancária Eletrônica, a contar da apresentação da nota fiscal/fatura pelo contratado, que deverá ser submetida ao atesto pelo setor competente pela fiscalização do contrato.

24. FISCALIZAÇÃO E ACOMPANHAMENTO
24.1 Todos os serviços executados pela empresa Contratada serão acompanhados e fiscalizados por servidores da Secretaria de Tecnologia da Informação e Comunicação (SETIC), com autoridade para exercer em nome do TJAM toda e qualquer ação de orientação geral, controle e fiscalização dos serviços.
24.2 As decisões e providências que ultrapassem a competência da Fiscalização deverão ser solicitadas aos seus superiores em tempo hábil para adoção das medidas convenientes;
24.3 A Contratada não poderá, em hipótese nenhuma, iniciar os serviços contratados, sem prévia emissão pela SETIC, da correspondente Ordem de Serviço.
24.4 Cabe à Fiscalização, entre outras atribuições:
24.4.1 Verificar a conformidade da execução dos serviços com as normas especificadas e se os procedimentos e materiais empregados são adequados para garantir a qualidade desejada dos serviços;

24.4.2 Ordenar à Contratada que corrija, refaça ou reconstrua as partes dos serviços executados com erros ou imperfeições, que estejam em desacordo com as especificações das normas técnicas.
24.5 A ação da fiscalização exercida pelo TJAM não desobriga a empresa Contratada de suas responsabilidades contratuais;
24.6 À fiscalização caberá o direito de rejeitar os materiais ou serviços que não satisfaçam aos padrões especificados nas normas técnicas e/ou especificações dos fabricantes.
24.7 O fiscal poderá suspender os serviços por descumprimento de exigências estabelecidas em normas ou padrões e projetos. Poderá, também, autorizar seu prosseguimento, verificada a correção da falha que ocasionou a suspensão.
24.8 A fiscalização do contrato, ao verificar que houve subdimensionamento da produtividade pactuada, sem perda da qualidade na execução do serviço, deverá comunicar à autoridade responsável para que esta promova a adequação contratual à produtividade efetivamente realizada, respeitando-se os limites de alteração dos valores contratuais previstos no § 1º, do artigo 65, da Lei 8.666, de 1993.
24.9 A conformidade do material/técnica/equipamento a ser utilizado na execução dos serviços deverá ser verificada juntamente com o documento da Contratada que contenha a relação detalhada dos mesmos, de acordo com o estabelecido neste Termo de Referência, informando as respectivas quantidades e especificações técnicas, tais como: marca, qualidade e forma de uso.
24.10. O representante da Contratante deverá promover o registro das ocorrências verificadas, adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais, conforme o disposto nos § 1º e 2º, do art. 67, da Lei n e 8.666, de 1993.
24.11 As atividades de gestão e fiscalização da execução contratual devem ser realizadas de forma preventiva, rotineira e sistemática, podendo ser exercidas por servidores, equipe de fiscalização ou único servidor, desde que, no exercício dessas atribuições, fique assegurada a distinção dessas atividades e, em razão do volume de trabalho, não comprometa o desempenho de todas as ações relacionadas à Gestão do Contrato.
24.12 A fiscalização técnica dos contratos avaliará constantemente a execução do objeto.
24.13 Durante a execução do objeto, o fiscal técnico deverá monitorar constantemente o nível de qualidade dos serviços para evitar a sua degeneração, devendo intervir para requerer à CONTRATADA a correção das faltas, falhas e irregularidades constatadas.
24.14. O fiscal técnico deverá apresentar ao preposto da CONTRATADA a avaliação da execução do objeto ou, se for o caso, a avaliação de desempenho e qualidade da prestação dos serviços realizada.
24.15 Em hipótese alguma, será admitido que a própria CONTRATADA materialize a avaliação de desempenho e qualidade da prestação dos serviços realizada.
24.16 A CONTRATADA poderá apresentar justificativa para a prestação do serviço com menor nível de conformidade, que poderá ser aceita pelo fiscal técnico, desde que comprovada a excepcionalidade da ocorrência, resultante exclusivamente de fatores imprevisíveis e alheios ao controle do prestador.
24.17 O fiscal técnico poderá realizar avaliação diária, semanal ou mensal, desde que o período escolhido seja suficiente para avaliar ou, se for o caso, aferir o desempenho e qualidade da prestação dos serviços.
24.18 A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade da CONTRATANTE ou de seus agentes, gestores e fiscais, de conformidade com o art. 70 da Lei n e 8.666, de 1993.

Manaus, data registrada no sistema.

Diogo Mendonça de Sousa	**Breno Figueiredo Corado**
Diretor da Divisão de Infraestrutura de TIC	Secretário de Tecnologia da Informação e Comunicação
SETIC/DVITIC	SETIC

Documento assinado eletronicamente por **DIOGO MENDONCA DE SOUSA**, **Diretor(a)**, em 18/07/2023, às 17:37, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **BRENO FIGUEIREDO CORADO**, **Secretário(a)**, em 19/07/2023, às 14:02, conforme art. 1º, III, "b", da Lei 11.419/2006.