permita a criação de políticas de liberação ou bloqueio baseando-se em aplicações web e URL.

2.4.5.1. A gerência das políticas de segurança de controle de aplicação e controle de URL's deverá ser realizada na mesma interface web de gerenciamento.

2.4.5.2. Deve ser possível configurar o bloqueio a sites e aplicações que representem um risco de segurança e estão categorizadas como, ao menos, spyware, phishing, botnet, spam, tor, anonymizer, hacking ou categorias semelhantes.

2.4.5.3. Deve ser possível configurar o bloqueio a sites com conteúdo inapropriado como, ao menos, sexo, violência, armas, jogos e álcool.

2.4.5.4. Deve configurar regras para permitir ou bloquear aplicações ou páginas da Internet por pelo menos:

a) Usuário ou grupo do Active Directory ou LDAP, e;
b) IP e/ou sub redes.

2.4.5.5. Deve ser possível configurar o bloqueio de compartilhamento de arquivos com origem usualmente ilegais como, por exemplo aplicações torrents e peer-to-peer.

2.4.5.6. Deve ser possível configurar manualmente o bloqueio de aplicações ou categorias de sites de aplicações indesejadas.

2.4.5.7. Deve ainda ser possível adicionar uma URL ou aplicação que não está na base de dados.

2.4.5.8. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

a) Permitir especificar política por tempo, com definição de regras para um

determinado horário ou período (horário, diário, mensal e anual);

b) Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;
c) 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 LDAP, via autenticação com tecnologia OpenLDAP, Active Directory e base de dados local;
d) Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
e) Suportar armazenamento, na própria solução, de URLs, evitando delay de comunicação/validação das URLs;
f) Bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção “Safe Search” esteja desabilitada no navegador do usuário;
g) Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja solução de software livre;
h) Suportar a criação de categorias de URLs customizadas;
i) Permitir a customização de página de bloqueio, e;
j) Deve ser possível limitar o consumo de banda de aplicações.
k) Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

    i - Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

    ii - Reconhecer pelo menos 5.000 (cinco mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail, e;

    iii - Deve ser possível realizar ou solicitar a recategorização de uma URL.

l) Deve descriptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2 e TLS 1.3.
m) Para inspeção SSL/TLS, ou HTTPS Inspection, a solução deve oferecer suporte ao Perfect Forward Secrecy (conjuntos de cifras PFS, ECDHE).
n) Para tráfego criptografado (SSL/TLS), deve decriptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;
o) A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação.
p) Deve ser possível customizar a forma que serão exibidas as mensagens para os usuários nas seguintes ações:
    i - Aceitar e informar;
    ii - Bloquear e informar, e;
    iii - Perguntar.

q) Deve ser totalmente compatível e integrada com a base de objetos e aplicações do Grupo I itens 1 a 7 (Solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) - Tipo I, Tipo II, TIpo III, Tipo IV e V), permitindo o uso de políticas semelhantes em todos os equipamentos, para que as unidades descentralizadas compartilhem com as diretrizes de navegação das Sedes.

2.4.6. Identificação de Usuários

2.4.6.1. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logging;

2.4.6.2. Toda a solução proposta deverá ser implementada com autenticação dos usuários integrada e suportar aplicações de políticas granulares com base em nome do usuário, departamento e grupos, integrados com a plataforma Microsoft AD utilizando protocolo SAML (Security Assertion Markup Language) LDAP, Radius ou base de dados local;

2.4.6.3. A solução deve identificar usuários das seguintes fontes:

a) Active Directory - o *gateway* de segurança deve realizar consulta aos servidores AD para obter informação dos usuários, e;
b) Autenticação via navegador - Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador.
c) Para LDAP é admissível o uso de agentes nas estações de trabalho e servidores

2.4.6.4. A identificação do usuário registrado no Microsoft Active Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

2.4.6.5. Na integração com o AD, a operação de cadastro deve ser realizada na própria interface web de gerência, de maneira simples e sem utilização de scripts de comando;

2.4.6.6. Deve suportar o recebimento eventos de autenticação de soluções NAC via Radius ou API's ou Syslog, para a identificação de endereços IP e usuários;

2.4.7. Funcionalidade de VPN Site-to-Site

2.4.7.1. A solução deve prover acesso seguro criptografado entre duas localidades através da Internet;

2.4.7.2. A solução deve suportar autenticação com senha ou certificado;

2.4.7.3. Deverá permitir a comunicação híbrida através de localidades que se comunicam diretamente utilizando a topologia "mesh", e outras em que se faz necessária a centralização do tráfego utilizando uma topologia "hub-and-spoke";

2.4.7.4. Deverá estabelecer túneis dinâmicos, entre spokes estritamente mediante interesse de tráfego (rotas aprendidas) e para a totalidade de localidades spokes;

2.4.7.5. No caso da topologia “*hub-and-spoke*”, deverá suportar mais de um ponto de concentração;

2.4.7.6. Deverá implementar de forma automatizada a constituição de túneis por meio da associação de perfis de configuração utilizando uma única interface gráfica;

2.4.7.7. A solução não deverá requerer configuração manual de endereçamento IP para a formação de túneis;

2.4.7.8. Deve suportar, pelo menos, criptografia AES 128 e 256;

2.4.7.9. Deve possuir mecanismo para monitorar a saúde do túnel remoto;

2.4.7.10. O dispositivo deverá suportar mecanismo de prevenção contra loop de roteamento entre camada overlay e underlay;

2.4.8. Funcionalidades do SD-WAN

2.4.8.1. Detecção de falha em links e redirecionamento automático do tráfego para links alternativos, baseado em, pelo menos, latência, jitter e perda de pacotes.

2.4.8.2. Monitoramento contínuo de parâmetros de latência, jitter e perda de pacotes.

2.4.8.3. Deve ser capaz de classificar os links nas seguintes categorias/tags:

a) Preferível: Utilizar um tipo link a não ser que outro com melhor performance esteja disponível;
b) Evitar: Utilizar o link somente o necessário, e;
c) Não utilizar o link;

2.4.8.4. Aplicação de políticas de roteamento com base em classificação de tráfego (DPI – Deep Packet Inspection ou análise de cabeçalhos), mapeamento de portas e domínios de destino.

2.4.8.5. Seleção de caminhos de acordo com características técnicas, evitando degradação da qualidade de serviço:

a) Parâmetros de qualidade: níveis aceitáveis de latência, jitter, perda, definida por SLA, e;
b) Métricas utilizadas: comparação dinâmica do estado atual do link com os demais links disponíveis, para múltiplos destinos.

2.4.8.6. Suporte a múltiplos tipos de conectividade WAN, incluindo MPLS, com links com IP dinâmico e links com IP Fixo.

2.4.8.7. Ajuste automático do encaminhamento de pacotes perante variações nas condições dos enlaces de comunicação, por métrica e aplicação.

2.4.8.8. No caso de falha de um enlace, todas as conexões existentes devem ser automaticamente transferidas (*statefully*) para o outro enlace que estiver ativo, sem a necessidade de intervenção do administrador;

2.4.8.9. Deve permitir acrescentar novos enlaces de comunicação ao firewall sem que haja a necessidade de alterar enlaces existentes;

2.4.8.10. Deve fornecer o recurso de balanceamento de carga e agregação da capacidade de banda de enlace para estabelecimento de túneis VPN somando a capacidades destes enlaces de comunicação para o tráfego de dados dentro da VPN. Os enlaces devem ser agregados de modo a somar as capacidades dos enlaces;

2.4.8.11. Deve possuir funcionalidades de agregação de VPN *site-to-site*, baseando-se em políticas de VPN (quando a política define se o tráfego deve ser

enviado via (VPN) ou com base em rotas, suportando topologias em hub e spoke ou full-mesh.

2.4.8.12. Deve ter a capacidade de realizar a seleção de links/agregação de links de forma dinâmica e automática;

2.4.8.13. A agregação de link deve possibilitar pelo menos dois modos:

a) Balanceamento de carga (*load sharing*): tráfego balanceado entre diferentes enlaces com base em medida de desempenho (tempo ao destino) ou banda relativa entre enlaces;
b) Deve ser possível a seleção de determinado link de comunicação em função da aplicação de rede sendo trafegada;
c) Deve realizar a seleção do link e estado de link (ativo/standby) em função de aplicação sendo usada na rede, e;
d) Deve ser possível decidir por qual link outbound o tráfego será encaminhado em função da aplicação transportada (aplicação identificada por meio de análise de conteúdo de pacote e não simplesmente por meio de análise de portas UDP/TCP).

2.4.8.14. Os equipamentos devem possuir mecanismos para facilitar a instalação onde seja possível carregar a configuração remotamente de um escritório central ou da nuvem, restringindo a necessidade de interação local para localidades remotas.

2.4.8.15. Deverá suportar convergência rápida de tráfego de um túnel ao outro, sem perda de sessões TCP ou UDP previamente estabelecidas.

2.4.8.16. Deverá suportar a comutação de tráfego entre circuitos de dados.

2.4.8.17. A solução deverá implementar medição automática da qualidade dos circuitos.

2.4.8.18. A solução deverá se adaptar aos problemas de rede e mitigá-los sem intervenção humana.

2.4.9. Provisionamento de Serviço

2.4.10. A solução deverá suportar a ativação dos dispositivos SD-WAN por meio de tecnologia "*Zero Touch provisioning*", sem requerer configuração manual local no equipamento a ser ativado.

2.4.11. A solução deverá suportar a ativação "*Zero Touch provisioning*" dos dispositivos SD-WAN.

2.4.11.1. A ativação e o provisionamento "*Zero Touch provisioning*" deverão ser realizados sem a necessidade de configuração prévia do dispositivo SD-WAN;

2.4.11.2. O provisionamento de serviços deverá ser feito por meio da interface gráfica da Gerência centralizada, não sendo aceito provisionamento por meio de interface de linha de comando ou CLI (*Command Line Interface*);

2.4.11.3. As comunicações de provisionamento deverão ser protegidas e criptografadas;

2.4.11.4. O fluxo de trabalho de provisionamento não deverá requerer o uso de ferramentas externas, além das já incluídas, exceto DHCP;

2.4.11.5. As alterações de configuração deverão ser registradas e armazenadas para fins de auditoria.

2.4.12. Qualidade de Serviço (QoS)

2.4.12.1. Deverá ser capaz de aplicar QoS nos pacotes tratados pela solução, inclusive para tráfego de voz, vídeo, streaming, videoconferência e web conferência;

2.4.12.2. A solução deverá suportar QoS para proteção do tráfego das aplicações prioritárias do cliente em cenários de congestionamentos dos circuitos.

2.4.12.3. Poderá permitir métodos de priorização de tráfego baseado em classes ou critérios, suportando no mínimo 3 tipos (ou similares).

2.4.12.4. Poderá utilizar mecanismo de priorização do tipo Fair Queuing, buscando utilizar toda a banda útil disponível para as aplicações, respeitando a classe de tráfego.

2.4.12.5. Poderá ser possível criar políticas de QoS com algum dos seguintes recursos:

a) Remarcação de DSCP;
b) *Traffic Shapping*, e;
c) QoS Hierárquico ou similar.

2.4.12.6. A solução deverá suportar QoS nos túneis.

2.4.12.7. Desejável que a solução permita integração com políticas de QoS DiffServ existentes na rede MPLS;

2.4.12.8. A solução deverá permitir limitar uso de banda por interface e aplicação;

2.4.12.9. A aplicação de QoS deverá ser customizável, possibilitando uma solução flexível, que reconhece a aplicação e aplica uma marcação de prioridade. Com base nessa marcação de prioridade encaminha o tráfego pela WAN mais adequada e, para algumas aplicações mais críticas, enviando o pacote por mais de um caminho;

2.4.12.10. Deverá permitir classificação e/ou direcionamento do tráfego utilizando no mínimo 6 (seis) dos seguintes parâmetros:

a) Endereços e/ou faixa de endereços IP (rede e/ou subrede);
b) Classes de serviço;
c) Aplicação que utilize DPI (Deep Packet Inspection);
d) Fully Qualified Domain Name (FQDN) ou classificação baseada em nome de domínio;

e) Porta TCP/UDP – Origem e Destino;
f) Internet Protocol v4 (IPv4) – Origem e Destino;
g) Differentiated Services Code Point (DSCP);
h) Uniform Resource Locator (URL) ou FQDN, e;
i) Aplicação de camada 7 (Microsoft 365, Microsoft Office, Microsoft Exchange, Microsoft Sharepoint, Microsoft Teams, etc.).

2.4.12.11. Os objetivos de qualidade de serviço (QoS) serão aplicados em cada Fluxo de Aplicação (*Aplication Flow*) por meio de políticas específicas configuradas no Orquestrador. Estas políticas deverão maximizar a experiência de navegação do usuário da rede e do serviço VPN, dentro dos limites impostos pela banda contratada, podendo atuar na priorização do tráfego.

2.4.12.12. Desejável permitir métodos de priorização de tráfego (QoS) por tipo de protocolo e por serviços da pilha TCP/IP, além de *Traffic Policing* e *Traffic Shaping*: *Priority Queuing* e *Generic Traffic Shaping* (GTS).

2.4.12.13. Desejável permitir que, mesmo com o link degradado, a solução trabalhe de forma inteligente, juntamente com seus protocolos, para que esta degradação seja praticamente imperceptível ao usuário final.

2.4.12.14. Usar probes artificiais baseadas em icmp, udp ou tcp para medir a qualidade da rede percebida pelo tráfego do usuário, medindo no mínimo jitter, latência e perda de pacotes.

2.4.12.15. Se houver necessidade de saída para internet via ponto remoto, deve ser possível selecionar por tipo de aplicativo.

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

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

2.4.12.18. Redistribuição do tráfego balanceado, de forma inteligente, entre os links utilizados, em caso de falhas nestes links, ou de acordo com as políticas de qualidade pré-definidas.

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

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

2.4.12.21. Desejável suportar políticas inteligentes usando configuração padrão de fábrica que executem redirecionamento automático e imposição de QoS de voz, vídeo e tráfego transacional

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

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

2.4.12.24. Suporte simultâneo ao redirecionamento do tráfego da Web de alguns aplicativos para a Internet centralizada, outros aplicativos para a Internet local.

2.4.13. Instalação equipamentos Grupo II itens 11, 12 e 13.

2.4.13.1. Caberá à contratada todo o processo de planejamento, a instalação, a configuração, a integração, os testes e a compatibilidade dos equipamentos, que deverão ser integrados à infraestrutura de Tecnologia de Informação existente no local de instalação dos equipamentos, como Switchs, roteadores, equipamentos servidores, entre outros.

2.4.13.2. Para compras de 1 até 20 equipamentos, a instalação deverá ocorrer em até 60 dias corridos após a comunicação da assinatura do contrato.

2.4.13.3. Para compras de mais de 20 equipamentos, a instalação deverá ocorrer em até 90 dias corridos após a comunicação da assinatura do contrato.

2.4.13.4. A contratada deverá disponibilizar o acompanhamento remoto durante a instalação de, pelo menos, um especialista, certificado pelo fabricante do equipamento, para ser responsável pela atividade de instalação, com, no mínimo, 40 horas de trabalho (sem contar a uma hora diária de almoço), sendo o limite de 9 horas diárias (incluindo uma hora para almoço), no horário das 8h às 17h;

2.4.13.5. Requisitos de Instalação

2.4.13.5.1. A instalação/migração não deve interromper as operações diárias da contratante sem agendamentos prévios e deve ser feita de forma a minimizar qualquer possível tempo de inatividade.

2.4.13.5.2. Eventuais necessidades de interrupção devem ser autorizadas e agendadas com a Administração do Órgão, com possibilidade de serem realizadas em finais de semana.

2.4.13.5.3. A instalação/migração envolverá as seguintes atividades:

a) Reunião de Alinhamento Inicial:

   i) A reunião de alinhamento inicial deverá ocorrer em até 15 dias da comunicação da assinatura do contrato.

b) Entrega do Plano de Trabalho (Cronograma e Escopo):

   i) O Plano de Trabalho deverá contemplar ao menos: Declaração de Escopo, Cronograma (datas da Instalação Física e Lógica e Efetiva entrada em produção dos novos equipamentos), Recursos Humanos, procedimentos e testes a serem realizados no final da instalação

   ii) O documento em PDF deverá ser enviado para o Gestor e o Fiscal Técnico em até 10 dias da reunião de alinhamento inicial.

   iii) A contratante terá 5 dias para analisar o documento, realizando, por

e-mail, as solicitações que entender cabíveis.

iv) Sendo necessárias alterações a contratada terá 5 dias para apresentar, também por e-mail, a versão final.

e) Execução da instalação e testes:

i) Esta etapa terá início após a entrega dos equipamentos e deverá ser concluída em até 60 dias da comunicação da assinatura do contrato para compras de 1 a 20 equipamentos.
Em até 90 dias da comunicação da assinatura do contrato para compras de 21 ou mais equipamentos.

ii) Fornecimento de todos os acessórios para as conexões elétricas e lógicas utilizadas, como cabos (rede, óticos e/ou elétricos) e materiais necessários para a sua fixação como parafusos, engates, trilhos, entre outros.

iii) Preparação remota dos equipamentos com sua última versão estável com seus patches (releases) mais recentes instalados. Não serão aceitas funcionalidades que estejam executando em builds não-estáveis (alpha, beta etc.) ou modificações personalizadas diretamente em código.

iv) Configuração lógica do equipamento para comunicação deste com a rede de dados da contratante.

v) Realização dos testes especificados no item 2.4.12.5.7.

vi) Ao final da etapa de Execução da instalação e testes, deverá ser enviado, para o e-mail do Gestor e do fiscal técnico, o arquivo de configurações dos novos equipamentos.

2.4.13.5.4. Quando o contratante também adquirir Clusters descritos no Grupo I itens 6 e 7 ou tiver instalado os itens de 1 a 5 do Grupo I, caso a contratante deseje, a transferência das configurações dos Clusters cabíveis para os Firewalls do tipo VI, VII e VIII, deverá ser realizada pela contratada;

2.4.13.5.5. Na instalação dos equipamentos, a contratada também deverá fazer a criação de novas regras e políticas que se mostrarem necessárias para a contratante.

2.4.13.5.6. Preferencialmente, o processo deverá ocorrer em ambiente apartado do ambiente produtivo;

2.4.13.5.7. Testes

No intuito de validar o funcionamento das configurações realizadas, incluindo migração, devem ser realizados, no mínimo, os seguintes testes:

a) Deverá ser feito, no mínimo, dois tipos de acesso a partir da rede interna.
   i) Acesso 1: utilizando protocolo https e sendo liberado o acesso, e;
   ii) Acesso 2: utilizando protocolo ssh e sendo bloqueado para a DMZ é liberado para a rede servidores;
e) Deverá ser feito um tipo de acesso externo com origem em um cliente VPN com destino a rede servidores.
f) Deverá ser exibido na console de gerência os registros que demonstrem:
   i) O horário da aplicação das últimas políticas;
   ii) A mudança realizada para bloqueio do Facebook;
   iii) O horário da mudança, e;
   iv) O administrador que realizou a mudança;

2.5. Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, por equipamento itens 11, 12 e 13 (Tipo VI, Tipo VII e Tipo VIII)

Entende-se apropriado apresentar um único conjunto de especificações para os serviços de garantia referente aos equipamentos do tipo VI, VII e VIII, porque a única alteração entre estes dois itens é a capacidade do produto em que o serviço será aplicado.

Assim, para os Firewalls dos Tipos VI, VII e VIII (Itens 11 a 13) deve a contratada oferecer, no mínimo, os serviços de garantia e atualização conforme segue.

2.5.1. Os serviços de assistência técnica “on-site”, realizados pela contratada ou

autorizados pela mesma mediante declaração expressa nas seguintes situações:

a) Quando atendimento remoto, deverão ser prestados no lugar onde o equipamento estiver instalado, em qualquer município do Brasil.
b) Quando atendimento para troca de peças e equipamentos com necessidade de presença física do técnico da contratada, nas Capitais e suas respectivas regiões metropolitanas.

2.5.2. Todos os custos e encargos relacionados à execução dos serviços de garantia e assistência técnica necessários durante o prazo de garantia dos serviços e dos bens serão de responsabilidade integral da contratada.

2.5.3. A contratada deverá prestar serviço de manutenção e suporte técnico ao longo da vigência do contrato destinado a:

e) Restabelecimento de serviços interrompidos ou degradados;
f) Solução de problemas de configuração e falhas técnicas nos serviços;
g) Esclarecimentos de dúvidas sobre configurações e utilização dos serviços, e;
h) Implementação de novas funcionalidades.

2.5.4. A garantia e serviço de assistência técnica do produto ofertados deverão ser do Fabricante.

2.5.5. A assistência técnica da garantia consiste na reparação das eventuais falhas dos equipamentos, mediante a substituição de peças, componentes e acessórios que se apresentem defeituosos de acordo com os manuais e normas técnicas específicas para os equipamentos. No caso do modelo do equipamento haver sido descontinuado, um similar será aceito, desde que possua as características técnicas iguais ou superiores às exigidas no Edital.

2.5.6. O serviço de garantia deverá abranger os defeitos de hardware e de software, através de manutenção preventiva ou corretiva, incluindo a substituição de peças, partes, componentes e acessórios, sem representar quaisquer ônus para o Tribunal.

2.5.7. Os equipamentos devem contar com garantia de funcionamento, atualização de assinaturas de proteção e suporte técnico local e remoto pelo fabricante, 24x7 (vinte e quatro horas por dia, sete dias na semana), pelo prazo de 60 (sessenta) meses, incluindo serviços de instalação e configuração, o qual poderá ser prestado pelo integrador (contratada) desde que possua pessoal qualificado e certificado pelo fabricante.

2.5.8. Todas as partes e peças deverão ser substituídas pelos serviços de garantia, através de funcionários habilitados e credenciados para tal. Não serão aceitos o envio de peças/equipamentos pelos Correios, para que haja substituição por parte do Contratante. O Contratante não se responsabiliza por quaisquer danos aos equipamentos, que possam vir a ocorrer caso seja utilizada a prática de postagem pelos Correios.

2.5.9. Toda e qualquer substituição de peças e componentes deverá ser acompanhada por funcionário designado pelo Contratante, que autorizará a substituição das peças e componentes, os quais deverão ser novos e originais.

2.5.10. Em caso de necessidade de nova instalação e/ou configuração os serviços deverão ser realizados pela Contratada ou pelo Fabricante, por técnico certificado com capacidade técnica para a realização do serviço comprovada através da apresentação de documento de certificação emitido pela própria fabricante do equipamento ou por empresa de treinamento reconhecida pelo fabricante. Se necessário, a documentação original ou “as built” deverão ser atualizados pela contratada.

2.5.11. Os serviços de suporte que porventura implicarem na necessidade de desligamento de outros equipamentos, como servidores, storage, links, etc., deverão ser executados, preferencialmente, em horários fora do expediente, podendo inclusive ocorrer em finais de semana ou feriados, a critério do contratante.

2.5.12. A contratada deverá ter acesso completo aos Fóruns de Produtos do fabricante durante a vigência do contrato;

2.5.13. A contratada deverá ter acesso à base de conhecimento de suporte online do fabricante durante a vigência do contrato;

2.5.14. A contratada deverá ter cadastrado em portal do fabricante para *download* de *firmwares*, *patches* e *softwares* que fazem parte ou complementam a solução;

2.5.15. Serão aceitos modelo de suporte híbrido, em que os primeiros níveis são atendidos pela contratada e os últimos níveis pelo fabricante.

2.5.16. Níveis de Gravidade dos chamados para definição de tempos de atendimento.

2.5.17.1. Gravidade 1

a) Um erro com impacto direto na segurança do produto;
b) Um erro isolado no software ou dispositivo em um ambiente de produção que torna o produto inoperante; por exemplo, impacto crítico no sistema, queda do sistema;
c) Um defeito relatado no produto em um ambiente de produção, que não pode ser razoavelmente contornado, em que haja uma condição de emergência que restrinja significativamente o uso, como por exemplo, PJe fora do ar por problemas de configuração do sistema Firewall;
d) Produto para de executar as funções de negócios necessárias, como interrupção no acesso à Internet via rede Interna; ou
e) Incapacidade de usar o equipamento ou qualquer outro impacto crítico na operação do Firewall que exija uma solução imediata.

2.5.17.2. Gravidade 2

a) Um erro isolado no software ou no equipamento que degrade substancialmente o desempenho dos sistemas de TIC que dependem dele, por exemplo, Sistema PJe acessível mas com performance muito degradada, lento e/ou com funcionalidades limitadas devido problemas de Firewall;

b) Um defeito que restringe o uso de um ou mais recursos mas não chega a afetar completamente o uso do Firewall, ou;

c) A utilização de uma função importante não está disponível e as operações são gravemente impactadas; por exemplo, lentidão nos sistemas da rede interna acessados via Internet.

2.5.17.3. Gravidade 3

a) Um erro isolado no Firewall que causa apenas um impacto moderado no uso do produto; por exemplo, Demora no login de sistemas via Internet, demora em algumas operações específicas do PJe, intermitência entre lentidão e desempenho satisfatório;

b) Um defeito que restringe o uso de um ou mais recursos do produto licenciado mas pode ser facilmente contornado, como parada do funcionamento da navegação Internet via rede Interna com autenticação de usuário e senha, mas que pode funcionar normalmente se liberada a autenticação até o problema ser resolvido, ou;

c) Um erro que pode causar algumas restrições funcionais, mas não tem um impacto crítico ou severo nas operações, como parada no acesso a sites de compra on-line.

2.5.17.4. Tempos de atendimento

Os tempos de atendimento estão descritos na tabela A4, conforme segue.

Tabela A4 - Tempos de atendimento o Serviço de atualização de garantia

Serviço	**Tempo e condições**
Regime do atendimento	24x7
Tempo de resposta comprometido para problemas de Gravidade 1 (1)	1hora e 30 minutos
Tempo de resposta comprometido para problemas de Gravidade 2 e 3 (1)	Gravidade 2 - 3 horas Gravidade 3 - 5 horas
Remessa de equipamentos em caso de necessidade de troca (RMA)	Próximo voo de saída/entrega expressa (quando aplicável) ou remessa no próximo

	dia útil (2)

(1) Entende-se cumprido o tempo de uma 1 hora e 30 minutos de tempo de atendimento caso haja comunicação em tempo real (chat, telefone). (2) Equipamentos são enviados durante o horário comercial normal e podem chegar fora do horário comercial.

2.5.18. A Contratada deverá providenciar o deslocamento de peças ou equipamentos para substituição bem como seu retorno sem qualquer ônus à contratante.

2.5.19. Todas as peças ou componentes utilizados/substituídos nos reparos deverão ser originais do fabricante, sem uso anterior e possuir, no mínimo, o mesmo desempenho e as mesmas garantias daqueles originalmente fornecidos.

2.5.20. Em caso de novos equipamentos, os mesmos devem ser compatíveis com os demais ativos de data center de cada Órgão participante. Ficará a cargo da contratada a verificação de compatibilidade antes da efetivação da reposição. Caso o sistema ofertado não tenha sua compatibilidade verificada, o correto funcionamento de todas as funcionalidades do sistema ofertado será de inteira responsabilidade da contratada, que deverá empreender todos os esforços necessários para entregar o sistema em pleno funcionamento, sob pena de arcar com as multas contratuais relativas a quebra de contrato.

2.5.21. Caso o equipamento não possa ser reparado dentro do prazo previsto, deverá ser providenciada pela contratada a instalação, em caráter provisório, de equipamento equivalente ou de configuração superior até que seja sanado o defeito do equipamento em reparo.

2.5.22. Caso os serviços de assistência técnica da garantia não possam ser executados nas dependências do contratante, o equipamento avariado poderá ser removido para o centro de atendimento da contratada. A contratada deverá fazer a justificativa por escrito relacionando os problemas apresentados que deverá ser apresentada ao setor competente do contratante que fará o aceite e providenciará a autorização de saída do equipamento, desde que o mesmo seja substituído por outro equivalente ou de superior configuração, durante o período de reparo. O

equipamento retirado para reparo deverá ser devolvido no prazo de 5 (cinco) dias úteis contados a partir da sua retirada.

2.5.23. A devolução de qualquer equipamento retirado para reparo deverá ser comunicada por escrito ao contratante.

2.5.24. A contratada deverá substituir o equipamento já instalado, por um novo e de primeiro uso, no prazo máximo de 2 (dois) dias corridos, na hipótese do mesmo equipamento apresentar defeito por 2 (duas) ou mais vezes dentro de um período de 20 (vinte) dias corridos.

2.5.25. Caso os equipamentos cobertos pelo serviço de garantia, atualização de assinaturas de proteção e suporte técnico vierem a ser declarados pelo fabricante em listas de *end-of-life*, *end-of-support* e/ou *end-of-sale* com essas datas terminando antes do período de vigência do contrato, os mesmos deverão ser substituídos pelos novos equipamentos indicados pelo fabricante em seu site, esses equipamentos devem ter capacidade idêntica ou superior ao equipamento antigo e possibilitar o uso de todas as funcionalidades do equipamento anterior.

2.5.26. Os serviços dependentes de atualização pela Internet e cujas licenças serão vinculadas à vigência do contrato, são: controle de acesso à Internet (controle de aplicações e filtragem de URLs), SD-WAN, prevenção de ameaças (IPS, Antivírus, Anti-Bot, Anti-Malware, Anti-Spyware), prevenção de perda de dados (data loss prevention) e postura dos *endpoints*, e demais funcionalidades necessárias para completa utilização dos equipamentos.

2.5.27. O licenciamento deverá permitir a utilização da solução, por tempo indeterminado, em sua última versão disponível na data do encerramento dos serviços de garantia, suporte técnico e atualização de versões.

2.6. Vigência e início do contrato

Os serviços de garantia e suporte terão vigência de 60 meses, com início a partir da emissão do termo de recebimento definitivo.

2.7. Itens 9 e 10 - Licenciamento de Serviço de *Software-Defined* WAN (SD-WAN) compatível com os equipamentos NGFW dos itens 1, 4 e 6 - Firewalls Tipo I e Tipo IV e dos itens 2 e 7 - Firewalls Tipo II e Tipo V

A solução de *Software-Defined* WAN (SD-WAN) deverá ser licenciada de forma a garantir um canal de comunicação seguro, utilizando a Internet, para conectar os Firewalls Centrais (em configuração de Cluster, dos tipos I, II, IV, V) aos Firewalls menores (dos tipos VI, VII e VIII).

Apesar de a compatibilidade do serviço de SD-WAN abranger os Firewalls dos tipos I, II, III, IV, V, VI, VII e VIII (Grupo I Itens 1 a 7 e Grupo II itens 11 a 13 do Edital), a habilitação desse serviço — seja por meio de licença ou componente de hardware adicional — aplica-se apenas aos Firewalls dos tipos I, II, IV e V. Isso ocorre porque os equipamentos dos tipos VI, VII e VIII (Itens 11 a 13 do Edital) já devem ter o serviço de SD-WAN ativado por padrão, sem a necessidade de aquisição separada. Já para o firewall tipo III não está prevista licença SD-WAN.

Uma unidade do Item 9 ou 10 corresponderá ao licenciamento SD-WAN para um cluster de equipamentos correspondente.

2.7.1. Vigência e início do contrato

Os serviços definidos nos itens 9 e 10 terão vigência de 60 meses, com início a partir da emissão do termo de recebimento definitivo da licença.

2.7.2. Requisitos mínimos para serviço de *Software-Defined* WAN (SD-WAN)

2.7.2.1. Após a solicitação do contratante a empresa terá até 15 dias para fornecer/habilitar o serviço.

2.7.2.2. A solução de SD-WAN deve ser parte da solução de segurança, com políticas comuns ao firewall principal, gerência e logs centralizados.

2.7.2.3. A solução deve permitir conexão entre os Firewalls via túnel criptografado (VPN *site-to-site*)

2.7.3. A solução deve permitir ao usuário da unidade remoto acesso à Internet diretamente, sem passar pelo Firewall principal da contratante, mas com as mesmas políticas de segurança, inspeção e filtro de conteúdo, de acordo com o seu perfil;

3. Grupo III - Solução de SASE (*Secure Access Service Edge*) e ZTNA (*Zero Trust Network Access*) na modalidade *Software* como serviço e Treinamento

Esta seção trata das especificações do grupo III itens 14 e 15 para a Solução de SASE (*Secure Access Service Edge*) e ZTNA *Zero Trust Network Access*.

3.1. Grupo III item 14 Licença de uso de solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Access) por usuário pelo período de 60 meses.

3.1.1. Características Gerais

3.1.1.1. As licenças de uso do SASE devem estar disponíveis para uso, integrada com a base de identificação de usuários do contratante, em até 60 dias da comunicação da assinatura do contrato.

3.1.1.2. O contrato terá vigência de 60 meses.

3.1.1.3. Anualmente, na data de aniversário do contrato, a contratada poderá redefinir o número de contas ativas, respeitando o mínimo de 200 contas e o teto definido no contrato.

3.1.1.4. A quantidade de licenças que devem ser inicialmente ativadas será informada à contratada no início do contrato. Essa quantidade deverá ser de no mínimo 200 (duzentas) licenças ativas. A solicitação precisará ser registrada por, no mínimo, e-mail.

3.1.1.5. Caberá à Contratante fazer o primeiro contato com a Contratada para saber a quantidade de licenças que deve ser enviada no primeiro pedido;

3.1.1.6. Caso seja solicitada a ativação de uma quantidade de contas inferior à quantidade máxima contratada, a diferença entre a quantidade de licenças solicitadas (ativas) e a quantidade de licenças contratadas será o saldo de licenças disponíveis, que não serão consideradas como ativas;

3.1.1.7. A Contratante poderá solicitar à Contratada, ajuste na quantidade de licenças, em múltiplos de 10, dentro do limite de licenças disponíveis no contrato. As licenças solicitadas comporão o total de licenças ativas para os próximos 12 meses. Esse processo poderá ser refeito a cada 12 meses;

3.1.1.8. Os ajustes anuais deverão respeitar o piso de 200 licenças e o teto definido em contrato.

3.1.1.9. Se a Contratada fornecer quantidade de licenças diferente da solicitada pela Contratante, caberá a Contratada arcar com os custos para regularizar a situação. A regularização da situação deverá ocorrer em até 15 dias corridos, contados da notificação da contratante.

3.1.1.10. Para efeito de pagamento, a quantidade total de licenças solicitadas será considerada como a quantidade de licenças ativas. O pagamento corresponderá ao número de licenças ativas.

3.1.1.11. As licenças só serão consideradas entregues quando estiverem disponíveis no console de administração e em acordo com a quantidade total solicitada;

3.1.1.12. Cada novo reajuste do quantitativo de licenças ativas deverá ser atendido em até 5 (cinco) dias úteis.

3.1.1.13. O contrato terá pagamento referente ao número de licenças definido na data da assinatura de contrato, ou na revisão anual do quantitativo, será efetuado **mensalmente, após a efetiva prestação dos serviços**, mediante apresentação de

nota fiscal/fatura correspondente e atestado de conformidade emitido pelo contratante, referente aos 12 meses seguintes de licença.

3.1.1.14. Todas as funcionalidades deverão ser ofertadas em nuvem, como serviço e por meio de um único agente instalado na máquina do usuário. A nuvem deverá ser distribuída globalmente, incluindo o Brasil e deverá ser licenciada por usuário, conforme quantitativo definido por cada participante;

3.1.1.15. A plataforma de segurança deverá ter ponto de presença no Brasil (Data Center), onde todos os usuários em território nacional terão suas transações processadas, incluindo todas as inspeções e aplicação de políticas de controle de acesso e segurança em tempo real;

3.1.1.16. O Data Center localizado no Brasil deverá ter rede independente com Sistema Autônomo e conectividade, redundante, em PTT (Ponto de Troca de Tráfego) no Brasil com peering com provedores de serviços, empresas de telecomunicações, CDNs (*Content Delivery Network*) e provedores de nuvem pública tais como (AWS, Microsoft e Google). Desta forma garantindo a melhor experiência e baixa latência aos usuários.

3.1.1.17. Não serão aceitos para solução SASE sistemas baseados em hardware ou software projetados para uso genérico, ou de código aberto (*open source*).

3.1.1.18. A solução de SASE deverá suportar todas as funcionalidades descritas neste certame no que tange controle de acesso e segurança à Internet e a aplicações SaaS por meio das seguintes opções de arquitetura de conectividade à plataforma de segurança:

a) Agentes instalados nas máquinas, e;
b) Utilização de proxy explícito via arquivos PAC (Proxy Auto-Configuration), neste caso com funcionalidades limitadas a acesso Web HTTP, HTTPS.

3.1.1.19. A solução de segurança, proteção de dados, controle de acesso à Internet e aplicações deverá fornecer disponibilidade de 99.999% ao ano;

3.1.1.20. Suportar geração de logs detalhados de acesso dos usuários Web, Aplicações Cloud, Bloqueios de Segurança e acessos;

3.1.1.21. Todas as inspeções e aplicações de políticas deverão ser realizadas na nuvem. Com exceção da verificação de postura, nenhuma inspeção de controle de acesso ou segurança deverá ser realizada na máquina do usuário;

3.1.1.22. A solução de segurança, proteção de dados e controle de acesso à Internet deverá oferecer suporte à criação de múltiplos administradores com privilégios distintos e segmentados;

3.1.1.23. No caso da utilização de agentes, a gestão de como o tráfego será encaminhado à plataforma, incluindo eventuais exclusões específicas (*bypass*), deverá ser gerenciada de maneira centralizada em uma console Web com o contexto de usuário e grupos de usuários. Não serão aceitas soluções que requeiram alteração ou customizações diretamente na máquina do usuário;

3.1.1.24. O agente único deve ser compatível com no mínimo os seguintes sistemas operacionais:

a) Windows 10 ou superior;
b) Linux kernel 6.6 ou superior;
c) MacOS 13 ou superior;
d) IOS 16 ou superior, e;
e) Android 12 ou superior.

3.1.1.25. Toda a solução proposta deverá ser implementada com autenticação dos usuários integrada e suportar aplicações de políticas granulares com base em nome do usuário, e grupos, integrados com a plataforma Microsoft AD utilizando protocolo SAML (*Security Assertion Markup Language*) e LDAP via OpenLDAP;

3.1.1.26. A solução de segurança deverá realizar, em uma única plataforma, sem passar por inspeção em múltiplos componentes de rede dentro da nuvem do

fabricante ou de terceiros, os controles de acesso e proteção de segurança para acesso à Internet e aplicações SaaS, consolidando capacidades de soluções de SWG e FWaaS;

3.1.1.27. Os mecanismos de inspeção da plataforma (URL *filtering*, Antivírus, etc) devem verificar todo o conteúdo dos pacotes de forma simultânea e em uma única abertura;

3.1.1.28. A solução deverá integrar-se nativamente e enviar em tempo real logs para plataformas de SIEM (*Security Information and Event Management*) possibilitando a integração com, no mínimo, as soluções de SIEM IBM Qradar e Trend One, ferramentas que compõe a solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos que compõem a Ata de Registro de Preços n.20/2024, vigente, resultante do Pregão Eletrônico n.30/2024 - PROAD n. 22.093/2024 do TRT 2, contratada por vários órgãos participantes do presente processo;

3.1.1.29. A solução deve ser capaz de fornecer a visualização de logs em tempo real;

3.1.1.30. A solução deverá armazenar os logs de auditoria por no mínimo 3 meses;

3.1.1.31. Os logs de auditoria devem conter no mínimo:

a) Ação: Login, Criação, Deleção;
b) Interface utilizada: API, Console Administrativa, e;
c) Categoria: Gerenciamento, Controle de Acesso, Gerenciamento de funções, Controle de acesso Web, Segurança Web e configurações avançadas.

3.1.2. Características para funcionalidades de SWG (*Secure Web Gateway*)

3.1.2.1. Suportar inspeção de SSL/TLS em 100% do tráfego Web, sem limites de volume de transações ou percentual inspecionado, em protocolos TLS 1.2 e 1.3,

para acesso do cliente SASE e os protocolos TLS 1.0, 1.1, 1.2, 1.3 para acesso às aplicações internas disponibilizadas;

3.1.2.2. Possibilidade de criar regras granulares de exceção a inspeção SSL/TLS, com base categorias de URL, host e domínios de destino, usuário, grupo ou departamento;

3.1.2.3. A solução deverá identificar automaticamente tráfegos Web em portas não padrão (80 e 443) e realizar a inspeção Web completa, incluindo inspeção SSL/TLS e todas as funcionalidades de controle de acesso e segurança, mesmo em uma arquitetura de proxy transparente;

3.1.2.4. Capacidade de criar filtros de URLs com base em categorias e subcategorias, que deverão ser atualizadas constantemente pelo fabricante;

3.1.2.5. Suportar a criação de categorias customizadas;

3.1.2.6. Suportar a criação e manutenção listas de URL via API;

3.1.2.7. A solução deve fornecer mecanismo para bloquear o acesso Web a destinos hospedados em determinados países. Este bloqueio deverá ser configurado de maneira simples, apenas selecionando os países que deseja bloquear;

3.1.2.8. Suportar o idioma Português do Brasil em páginas de erro e bloqueio apresentadas aos usuários, além de permitir customização;

3.1.2.9. A solução deverá ter capacidade de criar políticas Web, granulares, com critérios utilizando nome do usuário, grupos, departamento, categorias de URL, localidades para liberação ou bloqueio de upload e/ou download de arquivos de acordo com o seu tipo. Exemplo: EXE, RAR, PKG, XLS, PDF;

3.1.2.10. A solução deverá prover proteção de antivírus e antimalware com base em assinatura de arquivos. Esta proteção deverá ser realizada para download e upload, e a base de dados de assinatura ser atualizada constantemente pelo fabricante;

3.1.2.11. A solução deverá fornecer proteção contra ameaças avançadas, utilizando análise estática com base em reputação do domínio, origem, idade do domínio entre outras variáveis, além de uma análise dinâmica do conteúdo Web de 100% das requisições realizada a fim de detectar potenciais riscos aos usuários, tais como injeção de JavaScript malicioso, assinaturas de roubo de cookies XSS, conteúdos ativos maliciosos, conteúdos vulneráveis de ActiveX, Phishing dentre outras.

3.1.2.12. Deve possuir detecção e proteção de malwares para:

a) Todo tráfego Web de saída;
b) Inspeção dos seguintes protocolos: HTTP e HTTPS, e;
c) Adwares, Backdoor, Dialer, Downloader, Criptografado, Exploit, Hacktool, Heuristic, Keylogger, Infostealer, Packed, Potentially un-wanted applications, ransomware, rootkit, Spyware, Virus, Trojans e Worms.

3.1.2.13. A solução deverá ter atualizações constantes, minimamente diárias, de base de dados utilizada para bloqueio de segurança com base em reputação, prevenção a fraudes como Phishing, botnets, Command and Control, malware, spyware ou qualquer outro tipo de conteúdo malicioso;

3.1.2.14. A solução deverá detectar e bloquear assinaturas de ataques XSS (Cross Site Scripting) e de roubo de cookies dos usuários;

3.1.2.15. A solução deve monitorar e avaliar aplicações de comunicações unificadas, assim como o Teams e Zoom.

3.1.3. Características para funcionalidades de FWaaS (*Firewall as a Service*)

3.1.3.1. A solução deverá suportar capacidades de Firewall como serviço via agentes instalados nas máquinas dos usuários nas plataformas Windows, Linux, IOS, MacOS e Android;

3.1.3.2. A solução deve suportar, no mínimo, 350Mbps por túnel IPSEC;

3.1.3.3. Toda a inspeção e aplicação de política de Firewall, independente do método de implantação, deverá ser realizada na nuvem;

3.1.3.4. A solução deverá suportar a criação de regras de Firewall utilizando Destino, Protocolo udp/tcp e porta;

3.1.3.5. A solução deverá suportar como destino IP, Subredes ou endereços completos (FQDN);

3.1.3.6. A solução deverá suportar a criação de políticas de Web bloqueando o acesso a destinos em países específicos;

3.1.3.7. A solução deverá suportar criar regras, nos dois métodos de implementação com túneis ou agentes, com base em metadados do IdP como nome do usuário, grupos e departamento;

3.1.3.8. O FWaaS deverá ter capacidade de inspeção na camada 7, fazendo uso de tecnologia de DPI (*Deep Packet Inspection*), ou similar que entregue o mesmo caso de uso, para identificar nos primeiros pacotes a aplicação que está sendo utilizada;

3.1.3.9. A solução de FWaaS deverá possuir a capacidade de criar políticas específicas granulares para proteção de DNS;

3.1.3.10. A solução deverá suportar políticas de proteção de DNS granulares contendo, no mínimo, metadados do IdP (usuário, grupos e departamento), Localidades, Origem e Domínios Destino;

3.1.3.11. Para a proteção de DNS a solução deverá permitir ações como bloqueio ou redirecionar para um IP de BOTNETS para página de bloqueio;

3.1.3.12. A solução deverá ter proteção nativa contra ataques de DNS *Tunneling* que permita bloqueio de destinos maliciosos conhecidos, além de conter mecanismo de

detecção de assinaturas de ataques utilizando ferramentas conhecidas de DNS Tunneling como iodine, independente do domínio utilizado;

3.1.3.13. A proteção de DNS deverá permitir bloqueio via DNS, independente do protocolo da aplicação, de domínios com baixa reputação ou com histórico de ser malicioso para *Phishing*, Conteúdo Malicioso e utilizados para Botnets;

3.1.3.14. A solução deverá detectar e redirecionar requisições de DNS utilizando DOH (DNS over HTTPS), de forma transparente, para aplicação de políticas de DNS, detalhadas nos itens acima, Serão aceitas soluções que bloqueiem o DOH e realizem apliquem as políticas da resolução de DNS tradicional;

3.1.3.15. Assim como todo o escopo do FWaaS, a solução de proteção de DNS deverá suportar a implementação via agentes instalados nos dispositivos dos usuários;

3.1.4. Características para funcionalidades de visibilidade e controle de aplicações

3.1.4.1. A solução deverá identificar automaticamente uso de aplicações em nuvem (Cloud) pelos usuários, criando visibilidade em Dashboards e relatórios de Shadow IT;

3.1.4.2. O relatório de Shadow IT deverá permitir identificar uso de aplicações não sancionadas e com risco elevado, além de visualizar pela própria interface Web da solução quais usuários estão utilizando estas aplicações;

3.1.4.3. A solução deverá suportar a identificação e classificação entre aplicações sancionadas e não sancionadas pela contratante de, no mínimo, 4600 aplicações distintas. Esta base de dados deverá ser mantida e constantemente atualizada pelo fabricante e deverá conter, no mínimo, a categoria da aplicação;

3.1.4.4. A solução deverá permitir a criação de políticas de acesso com base na classificação da aplicação SaaS realizada pela contratante entre sancionadas e não sancionadas e índice de risco da aplicação;

3.1.4.5. A solução deverá suportar criar políticas granulares com critérios utilizando usuário, grupo, departamento, localidade e ações específicas nas aplicações SaaS. Como por exemplo, aplicações de compartilhamento de arquivos ter as opções de *Upload* e *Download* como critério, em aplicações como Webmail, ter as opções de Leitura e Envia de e-mails como critério;

3.1.5. Características para funcionalidades de Monitoramento da Experiência do Usuário

3.1.5.1. A solução deverá realizar monitoramento sintético a partir da máquina do usuário final, com testes de página Web e de Rede;

3.1.5.2. A console de gerenciamento deverá ser Web, e ter toda a configuração de forma centralizada;

3.1.5.3. A execução dos testes não deverá impactar o usuário final e deverá ser realizada em segundo plano, sendo transparente e imperceptível;

3.1.5.4. Quando executado testes de Web e Rede da mesma aplicação, por exemplo, Microsoft Teams, a solução deverá consolidar as métricas e apresentar uma única visão da experiência do usuário ao utilizar a aplicação SaaS;

3.1.5.5. A solução deverá apresentar Dashboards com o status das aplicações;

3.1.5.6. A Geolocalização deverá ser feita de maneira automática e transparente, sem nenhuma entrada de dados manual;

3.1.5.7. Caso o usuário esteja dentro de localizações conhecidas da solução de SWG e FWaaS, a solução deverá identificar que se trata de uma localidade conhecida;

3.1.5.8. Os testes e coleta de dados deverão acontecer no máximo a cada 15 (quinze) minutos;

3.1.5.9. A solução deverá coletar no mínimo as seguintes métricas de experiência:

a) Métricas Web:
   i - Tempo de resposta do Servidor;

b) Métricas do dispositivo do usuário:
   i - Consumo de CPU;
   ii - Qualidade do sinal Wi-Fi;
   iii - Memória;
   iv - Sistema Operacional, Descrição do hardware, IP público e IP externo utilizado;

3.1.5.10. Utilizando as métricas do dispositivo do usuário, a solução deverá ter um mecanismo simples de identificar a experiência do usuário em uma aplicação;

3.1.5.11. A solução deverá suportar o monitoramento de Websites na Internet e aplicações SaaS;

3.1.5.12. A solução deverá suportar a criação de alertas customizáveis com notificação por email;

3.1.5.13. A solução deverá manter o histórico da experiência de todos os usuários, por no mínimo 24 (vinte e quatro) horas;

3.1.6. Acesso a Aplicações Privadas

3.1.6.1. A solução deverá fornecer acesso remoto a aplicações e recursos internos da contratante, com segurança, validação de identidade, tunelamento encriptado, segregação de aplicações, verificação de postura e conexão direta com privilégio mínimo;

3.1.6.2. Deve permitir a conexão de no mínimo 500 usuários remotos de forma simultânea por órgão participante;

3.1.6.3. A solução deve habilitar uma arquitetura de privilégio mínimo, Zero Trust, definindo uma política de acesso granular para fornecer às pessoas certas no contexto certo, o acesso menos privilegiado aos aplicativos ou recursos e reduzir a superfície de ataque.

3.1.6.4. A solução deverá ser na nuvem e ter apenas o componente que irá viabilizar a conexão (conector ou publicador) instalado dentro do Data Center da contratante em uma, ou mais, máquinas virtuais.
Este componente interno ao Data Center deve seguir as seguintes características:

a) Não ter uma superfície de ataque exposta na Internet, não tendo nenhum IP público ou nenhuma necessidade de conexões de entrada da Internet para o componente;
b) Toda a conexão deverá ser apenas de saída, do componente com destino a nuvem do fabricante;
c) Cada instância de conector ou publicador deverá suportar no mínimo 500mbps de banda passante para acesso às aplicações internas;
d) Os conectores ou publicadores deverão atualizar suas versões de forma automática e realizar suas atualizações em janelas pré-definidas pela contratante (ex: Domingo às 4 AM) de forma 100% automatizada, sem causar interrupção dos serviços e sem intervenção do administrador;
e) Permitir ser instalado de forma flexível em qualquer ponto da rede da contratante, como por exemplo atrás de uma NAT (*Network Address Translation*);
f) Não criar um ponto único de conexão à rede da contratante, sendo possível a implementação de múltiplos conectores ou publicadores em pontos da rede, data centers ou nuvem distintas, fornecendo ao usuário o acesso direto aos recursos com menor latência possível de forma dinâmica;
g) Permitir o usuário a conectar em aplicações distintas simultaneamente utilizando conectores ou publicadores em pontos da rede distintos, priorizando sempre a melhor experiência do usuário;
h) Os conectores ou publicadores deverão ser independentes, não exigindo conectividade interna completa a todos os recursos privados. Sendo possível,

por exemplo, fornece acesso a aplicações ou recursos simultaneamente aos usuários em múltiplos Data Centers ou Nuvem, mesmo que estes Data Centers ou Nuvem não tenham conexão entre eles, e;

i) A solução deverá autenticar o usuário em um provedor de identidade (IdP) e com base em identidade, políticas granulares, segmentação de aplicações e posturas específicas fornecer acesso a aplicações Web, ou qualquer outra com protocolo TCP e UDP, tais como (SSH, RDP, SQL, Aplicações Client-to-Server, Compartilhamento de Arquivos, etc) de forma transparente, sem a necessidade de alteração do cliente original da aplicação, criando um túnel encriptado que conectará o usuário até a aplicação e não a rede da contratante.

3.1.6.5. A solução não deve operar como uma VPN, fornecendo um IP da rede local, e sim, conectar o usuário direto aos recursos e aplicações via túneis encriptados específicos, sempre após validação de política de identidade, postura e políticas de acesso;

3.1.6.6. Os usuários remotos não devem possuir visibilidade de aplicativos não autorizados. Os recursos não autorizados não devem apenas ser inacessíveis, mas também completamente invisíveis;

3.1.6.7. A definição de aplicações ou segmentos de aplicações deverá ter a flexibilidade de suportar hostname (FQDN), IP ou domínio com wildcard, como por exemplo (*.rede.local)

3.1.6.8. Fazer com que cada solicitação do usuário flua por meio de políticas contextuais para autenticação e autorizações consistentes, além de fornecer um ponto de monitoramento e registro unificado;

3.1.6.9. Utilizar túneis encriptados TLS ou DTLS, versão 1.2 ou 1.3;

3.1.6.10. Todas as comunicações entre os componentes da solução e a infraestrutura em nuvem do fabricante devem mutuamente utilizar certificados pinados ou IPSEC;

3.1.6.11. A solução deve ser blindada contra-ataques de “Man-in-the-middle” (MITM), aceitando-se que a blindagem contra MITM seja via IPSEC;

3.1.6.12. Suportar múltiplos provedores de identidade (IdP - Identity Provider) e múltiplos domínios, na mesma instância e console de gestão, que suporte autenticação utilizando protocolo SAML 2.0 e LDAP. Viabilizando desta forma, acesso seguro a outras unidades de negócio e terceiros a recursos privados da contratante, além de possibilitar a simplificação e modernização da conectividade e integrações futuras;

3.1.6.13. Permitir a descoberta automatizada de novas aplicações que não foram previamente provisionadas aos usuários explicitamente;

3.1.6.14. Trazer o monitoramento da atividade dos usuários, dando às equipes de TI formas de monitorar e gerenciar facilmente todas as atividades de forma granular, entendendo, no mínimo, qual usuário, quando, qual aplicação, qual política autorizou ou negou o acesso, status da postura e localização do usuário;

3.1.6.15. A solução deverá suportar envio, em tempo real, das informações do item anterior para uma plataforma de SIEM, possibilitando a integração com, no mínimo, as soluções de SIEM IBM Qradar e Trend One, ferramentas que compõe a solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos que compõem a Ata de Registro de Preços n.20/2024, vigente, resultante do Pregão Eletrônico n.30/2024 - PROAD n. 22.093/2024 do TRT 2, contratada por vários órgãos participantes do presente processo;

3.1.6.16. A solução deve usar o painel Web para criar e editar políticas com facilidade. O portal de gestão central deve trazer:

a) Controle de acesso centralizado;
b) Gestão de políticas;
c) Configuração de postura;

d) Registro de atividades detalhados e seus metadados contendo, no mínimo, usuário, localidade, postura, IP de origem, aplicação destino, política de acesso que concedeu ou negou o acesso;
e) Status da estrutura que suporte a solução como conectores ou publicadores;
f) Status do processo de atualização automatizada dos conectores e publicadores, e;
g) Status das aplicações que deverão ser monitoradas e se estas estão disponíveis ou não.

3.1.6.17. Suportar a configuração de qualquer aplicação TCP ou UDP com tráfego originado pelo usuário de forma transparente, sem nenhuma alteração ou customização no seu cliente original;

3.1.6.18. Permitir o agrupamento de aplicações ou recursos para facilitar a criação de políticas (ex: Aplicações Administrativas);

3.1.6.19. Suportar a gestão de políticas de acesso via API;

3.1.6.20. Suportar diferentes tipos de validação de postura. O suporte a cada tipo pode variar dependendo da plataforma (Windows, Mac, Linux), sendo requerido que deverá suportar, no mínimo, 2 (dois) dos tipos de postura listadas abaixo por plataforma:

a) Validação da presença de um Antivírus;
b) Validação de Certificado Cliente (chave privada e pública) assinada por um CA específico;
c) Validação de Certificado confiável no dispositivo;
d) Validação de qualquer processo executando na máquina, incluindo a validação da assinatura do seu fabricante;
e) Validação de máquina no domínio;
f) Validação de disco encriptado;
g) Validação de Registro de chave no Windows, e;
h) Validação de presença de um arquivo.

3.1.6.21. Exigência de uma versão mínima do Sistema Operacional;

3.1.6.22. Detectar alterações Jail Break (IOS) e rooted (Android).

3.1.6.23. A solução deverá ter mecanismos de proteção e políticas granulares de postura para cada acesso à aplicação. Desta maneira permitindo criar maiores restrições a aplicações mais críticas ao negócio e menos restritas a aplicações de suporte a TI.

3.1.7. Ferramenta de iscas digitais (Deception)

3.1.7.1. A solução deve possuir módulo de defesa ativa para detecção de ameaças na rede interna e externa;

3.1.7.2. Exclusivamente para o módulo de defesa ativa será aceita composição de soluções terceiras para o completo atendimento;

3.1.7.3. A solução proativa deve ser capaz de espalhar iscas no ambiente a fim de enganar o atacante;

3.1.7.4. A solução deve permitir a instalação de um conector no ambiente da contratante capaz de criar "iscas" falsas em várias redes locais (VLAN's);

3.1.7.5. Possuir iscas de rede capazes de detectar atividades de varredura e movimentação lateral;

3.1.7.6. Permitir a instalação de agentes nos Endpoints da contratante possibilitando a criação de arquivos, processos e credenciais falsas;

3.1.7.7. Capacidade de" imitar" ativos reais da rede a fim de enganar o atacante;

3.1.7.8. A solução deve ser licenciada para no mínimo 20 Iscas/Chamarizes ou VLANs;

3.1.7.9. Possuir, pelo menos, os seguintes tipos de Iscas/Chamarizes:

a) Iscas de Rede: Espalhadas em segmentos de rede específicos;
b) Iscas no Active Directory: Criação de usuário e computadores falsos, e;
c) Iscas nos Endpoints: Criação de arquivos, aplicações e credenciais falsas.

3.1.7.10. Deve ser capaz de mostrar um sumário de todas as iscas espalhadas dentro do ambiente e o status de operação;

3.1.7.11. Deve possuir Iscas de inteligência externas que devem ser apontadas no DNS externo da contratante;

3.1.7.12. A solução deve ser capaz de detectar e mapear ocorrências de acordo com framework MITRE ICS.

3.1.7.13. O módulo de defesa ativa deve fornecer uma visão geral de forma temporal das atividades detectadas pela plataforma;

3.1.7.14. A solução deve fornecer uma visão geral temporal das atividades detectadas ao longo do tempo e ao longo da semana;

3.1.7.15. Deve permitir analisar eventos passados permitindo customização da janela de tempo;

3.1.7.16. A solução deve fornecer uma barra de consulta usada para filtrar os eventos detectados pela plataforma;

3.1.7.17. Dentre as formas de pesquisa a solução deve ser capaz de filtrar no mínimo as seguintes informações:

a) Endereço IP do Atacante;
b) IP de Destino;
c) Porta de destino;
d) Duração da conexão;
e) Score de Risco do atacante;

f) Protocolo de rede;
g) Fase do Kill Chain, e;
h) Tipo da isca;

3.1.7.18. A solução deve ser capaz de exportar evidências coletadas pelas iscas em pelo menos um dos seguintes formatos:

a) RDP;
b) IOCs;
c) PCAP e;
d) STIX, que é um padrão para representar e compartilhar informações sobre ameaças cibernéticas de forma estruturada e automatizada.

3.2. Item 15 - Voucher de Treinamento para solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Access)

3.2.1. O Treinamento fornecerá uma compreensão dos conceitos básicos e das habilidades necessárias para configurar o sistema previsto no item 17 do Edital da presente licitação.

3.2.2. O curso deverá abordar configurações de políticas de SASE (*Secure Access Service Edge*) e ZTNA (*Zero Trust Network Access*), gerenciamento e monitoramento da solução, atualizações e configurações de soluções de SASE e ZTNA.

3.2.3. O Treinamento deverá ser fornecido na forma de voucher[6] individual para treinamento;

3.2.4. A duração do treinamento deve ser de, no mínimo, 20 horas aula distribuídas em até 5 dias úteis, com um máximo de 8 horas aula por dia;

[6] Para o objeto definido nos itens 8 e 15 da presente contratação, o Voucher é um vale, ou valor em crédito, para realização de Treinamento dentro de plataforma de educação à distância, que deve ser disponibilizado em turmas regulares dentro de um período específico de tempo.

3.2.5. O treinamento e o material didático deverão ser em língua portuguesa;

3.2.6. O treinamento deverá ocorrer no período entre 8h00 e 18h00;

3.2.7. As turmas deverão ter até 15 alunos;

3.2.8. O treinamento deverá ser realizado de forma on-line e síncrona;

3.2.9. Deverá ser fornecido certificado de conclusão do treinamento em até 10 dias após sua conclusão, contendo:

a) Nome do Aluno;
b) Nome do Curso;
c) Carga horária do Curso;
d) Data de início e fim do Curso;
e) Nome e assinatura do emissor, e;
f) Linguagem em Português do Brasil. Mesmos os certificados oficiais do fabricante.

3.2.10. As turmas para os cursos devem estar disponíveis para as contratantes em até 30 dias corridos após a comunicação da assinatura de cada contrato de aquisição de vouchers.

3.2.11. Devem haver turmas regulares até 12 meses depois da data da comunicação da assinatura de cada contrato.

3.2.12. A contratante deve ser comunicada mensalmente das turmas regulares e pode comunicar o uso do voucher do curso até, no mínimo, 15 dias antes do início da turma.

3.2.13. Conteúdo programático:

a) Características e funcionalidades básicas da solução;
b) Funcionalidades e operação de SWG (Secure Web Gateway);

c) Funcionalidades e operação de FWaaS(Firewall as a Service);
d) Visibilidade e controle de aplicações;
e) Configuração e análise da Experiência do Usuário;
f) Acesso e configuração das aplicações privadas, e;
a) Configuração de ZTNA, configuração de políticas de postura para clientes Windows e Linux. Substituição de VPN cliente por ZTNA benefícios e diferença entre os conceitos.

4. Grupo IV - Serviço Gerenciado Mensal

4.1. Itens 16, 17 e 18 - Serviço gerenciado mensal, contendo operação assistida, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos Grupo I (itens 1, 4 e 6) - Tipo I e Tipo IV, Grupo I (itens 2 e 7) - Tipo II e Tipo V e Grupo I (itens 3 e 5) - Tipo III

Especificação completa dos itens 16 a 18, Serviço Gerenciado com tratamento de incidentes para Cluster de equipamentos do Tipo I, II, III, IV e V.

Importante: Para contratar o serviço gerenciado, o órgão deve, obrigatoriamente, possuir/adquirir o cluster correspondente com suporte e garantia ativos (Itens 1 a 7).

Entende-se também apropriado apresentar um único conjunto de especificações para os serviços gerenciados dos itens 16 a 18 porque, neste processo, a diferença entre estes itens é o tipo de equipamentos em que o serviço será aplicado, conforme segue:

- Item 16 - Cluster de equipamentos do Grupo I (itens 1, 4 e 7) - Tipo I e Tipo IV;
- Item 17 - Cluster de equipamentos do Grupo 1 (itens 2, 5 e 8) - Tipo II e Tipo V;
- Item 18 - Cluster de equipamentos do Grupo I (itens 3 e 6) - Tipo III;

Como cada serviço gerenciado é ligado a um tipo/grupo de equipamentos, caso o Órgão participante possua mais de um Cluster de equipamentos Firewall deverá adquirir quantitativo de mais de um item do grupo.

4.1.1. Serviço Gerenciado de Administração, Operação e Suporte da Solução

4.1.1.1. Características Gerais

Os serviços gerenciados devem fornecer suporte técnico avançado em segurança de redes para solução de Firewall de próxima geração, de forma pró ativa, ou seja, tomando a iniciativa de ajustes e combate a invasões, em regime 24x7 (vinte quatro horas por dia e sete dias por semana), incluindo finais de semana e feriados).

O serviço tem especial valor por conter monitoramento e possibilidade de atuação quando não há equipe do contratante em operação, ou seja, fora do expediente.

A contratada deve atuar, no mínimo, nas seguintes situações:

a) Ataques de dia zero (*zero-day*);
b) Extração de ameaças;
c) Antivírus;
d) Anti-bot;
e) IPS;
f) Controle de aplicativos;
g) Filtragem de URL e reconhecimento de identidade, e
h) SD-WAN (quando a contratada adquirir o item 11,12 e/ou 13).

Os serviços de operação e sustentação abrangem atividades que não são cobertas pela garantia ou pelo suporte técnico do fabricante, visto que esses visam garantir a resolução de problemas referentes a falhas e defeitos nos equipamentos ofertados, enquanto aqueles visam fundamentalmente viabilizar a administração e a operação de tais equipamentos.

Os serviços de operação e sustentação não abrangem as atividades referentes à primeira instalação e configuração inicial dos equipamentos ofertados.

4.1.1.2 O serviço gerenciado para atendimento de ocorrências deve acontecer no regime 24x7x365. Ou seja, 24 horas por dia, sete dias por semana, 365 dias por ano, incluindo feriados;

4.1.1.3. Monitoramento remoto do ambiente do contratante em regime 24x7 através de plataforma de gerência do fabricante, com, no mínimo:

a) Tratamento de falsos positivos e de falsos negativos;
b) Interpretação de resultados em análises de detecções;
c) Emissão de relatórios técnicos e executivos contemplando, ao menos, o nível de aderência à solução e ameaças detectadas;
d) Análise forense dos eventos adversos que ocorrerem e forem detectados pela solução;
e) Atuação na investigação e contenção de ameaça relacionada à detecção de evento adverso;
f) Envolvimento da equipe técnica da contratante no tratamento de eventos adversos.

4.1.1.4. Relatórios com frequência mensal apresentando, no mínimo:

a) O diagnóstico do sistema de Firewall (*health check*);
b) Resumo dos chamados tratados no mês, e;
c) A listagem dos últimos acessos de nível administrativo.

4.1.1.5. Requisição de Mudança para configuração de Regras e Criação de Redes Virtuais Privadas (VPN);

4.1.1.6. Atualização de Firmware dos equipamentos[7];

4.1.1.7. Auxílio na substituição de produtos[8];

[7] Desde que haja contrato de atualização do produto vigente e em nome do contratante.
[8] Desde que haja contrato de suporte do fabricante, prevendo troca de equipamentos, vigente e em nome do contratante.

4.1.1.8. Prever, no mínimo, 10 horas por mês de Serviço de suporte de nível 2 e 3 do fabricante.

4.1.1.9. Deve contemplar atuação pró-ativa, por meio da administração e operação diária da solução e pelo contato entre as equipes técnicas da contratada e da contratante, enquanto a atuação reativa será realizada por meio da abertura de chamados pela equipe técnica da contratante, para os quais contarão os Níveis Mínimos de Serviço;

4.1.1.10. Os métodos de atuação serão acessos remotos e efetuados via VPN fornecida pelo contratante;

4.1.2. Vigência e início do contrato

Os serviços gerenciados terão vigência de 60 meses, iniciando em até 15 dias da comunicação da assinatura do contrato.

4.2. Item 19 - Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, sem alta disponibilidade por equipamentos do Grupo II (itens 11, 12 e 13) - Tipo VI, Tipo VII e Tipo VIII

4.2.1. Serviço Gerenciado de Administração, Operação e Suporte da Solução com resposta a incidentes

4.2.1.1. Características Gerais

Os serviços gerenciados devem fornecer suporte técnico avançado em segurança de redes para solução de Firewall de próxima geração nos equipamento do Tipo VI, VII e VIII, de forma pró ativa, ou seja, tomando a iniciativa de ajustes e combate a invasões, em regime 24x7 (vinte quatro horas por dia e sete dias por semana, incluindo finais de semana e feriados).

O serviço tem especial valor por conter monitoramento e possibilidade de atuação quando não há equipe do contratante em operação, ou seja, fora do expediente.

A contratada deve atuar, no mínimo, nas seguintes situações:

a) Ataques de dia zero (*zero-day*);
b) Extração de ameaças;
c) Antivírus;
d) Anti-bot;
e) IPS;
f) Controle de aplicativos;
g) Filtragem de URL e reconhecimento de identidade, e;
h) SD-WAN

4.2.1.2. O serviço gerenciado para atendimento de ocorrências deve acontecer no regime 24x7x365. Ou seja, 24 horas por dia, sete dias por semana, 365 dias por ano, incluindo feriados;

4.2.1.3. Monitoramento remoto do ambiente do contratante em regime 24x7 através de plataforma de gerência do fabricante, com, no mínimo:

a) Tratamento de falsos positivos e de falsos negativos;
b) Interpretação de resultados em análises de detecções;
c) Análise dos eventos relacionados a rede SD-WAN, com fornecimento de soluções ou melhorias dos controles aplicados;
d) Emissão de relatórios técnicos e executivos contemplando, ao menos, o nível de aderência à solução e ameaças detectadas;
e) Análise forense dos eventos adversos que ocorrerem e forem detectados pela solução;
f) Atuação na investigação e contenção de ameaça relacionada à detecção de evento adverso, e;
g) Envolvimento da equipe técnica da contratante no tratamento de eventos adversos.

4.2.1.4. Relatórios com frequência mensal apresentando, no mínimo:

a) O diagnóstico do sistema de SD-WAN (*health check*);
b) Resumo dos chamados tratados no mês, e;
c) A listagem dos últimos acessos de nível administrativo.

4.2.1.5. Requisição de Mudança para configuração de Regras e Criação de Redes Virtuais Privadas (VPN).

4.2.1.6. Atualização de Firmware dos equipamentos[9].

4.2.1.7. Auxílio na substituição de produtos[10];

4.2.1.8. Deve contemplar atuação pró-ativa, por meio da administração e operação diária da solução e pelo contato entre as equipes técnicas da contratada e da contratante, enquanto a atuação reativa será realizada por meio da abertura de chamados pela equipe técnica da contratante, para os quais contarão os Níveis Mínimos de serviço;

4.2.1.9. Os métodos de atuação serão acessos remotos e efetuados via VPN fornecida pelo contratante;

4.2.1.10 O serviço deverá ser prestado em língua portuguesa.

4.2.2. Vigência e Início do Contrato

Os serviços gerenciados terão vigência de 60 meses, iniciando em até 15 dias da comunicação da assinatura do contrato.

4.3. Nível Mínimo de Serviço Para o Grupo IV - Serviço gerenciado mensal para equipamentos Firewall (Itens 16 a 19)

---

[9] Desde que haja contrato de atualização do produto vigente e em nome do contratante.
[10] Desde que haja contrato de suporte do fabricante, prevendo troca de equipamentos, vigente e em nome do contratante.

Os Níveis Mínimos de Serviço e severidades dos chamados para os Grupo IV, itens 16 a 19 são definidos na tabela TR5, a saber:

Tabela A5 - Níveis Mínimos de Serviço para Serviço Gerenciado

Severidade	Descrição	Prazo de Início de atendimento	Desconto por descumprimento (3)	Prazo de solução	Desconto por descumprir (3)
1 - Alta	Indisponibilidade total da solução, problema generalizado no ambiente tecnológico causado pela solução	2 horas a contar da abertura do chamado	1 % de desconto por hora adicional, limitado a 6 horas de atraso.	6 horas a contar da abertura do chamado	1% de desconto por hora adicional, limitado a 24 horas de atraso.
2 - Média	Falha, simultânea ou não, de uma ou mais funcionalidades, que não cause indisponibilidade, mas que apresente problemas de funcionamento e/ou desempenho da solução ou no ambiente tecnológico	4 horas a contar da abertura do chamado	0,2% de desconto por hora adicional, limitado a 24 horas de atraso.	NBD(1) + 1 dia útil (2)	0,2% de desconto por hora adicional, limitado a 96 horas de atraso.
3 - Baixa	Instalações, configurações, atualizações de versões, dúvidas dentre outros	NBD	0,1% de desconto por hora adicional, limitado a 48 horas de atraso.	NBD + 2 dias úteis	0,1% de desconto por hora adicional, limitado a 192 horas de atraso.

(1) NBD é uma sigla em inglês que significa Next Business Day, ou seja, próximo dia útil. (2) Serão considerados dias úteis todos os dias, com exceção de sábados, domingos e feriados nacionais. (3) O valor de referência para o desconto será o valor mensal pago pelo conjunto do serviço gerenciado. (4) A medição dos Níveis mínimos de serviço será feita mensalmente.

A contratante, a seu critério, poderá fornecer seu login e senha de acesso ao site do fabricante para que a equipe técnica da contratada possa responder pelo Regional nas interações referentes à garantia dos equipamentos. Nesses casos, a contagem do tempo de atendimento estipulada em contrato deverá ser suspensa, quando o chamado depender de ação do fabricante, especialmente quando for necessária a troca de equipamentos, a fim de evitar prejuízo por atraso que não seja de responsabilidade da contratada.

A impossibilidade de registro de chamados em qualquer horário contratado deverá ser considerada descumprimento do nível mínimo de serviço com severidade 1.

Anexo II - Quantitativos dos itens dos participantes da aquisição de Solução de NG Firewall coordenada pelo TRT12 em 2025 - Atualizada em 28/8/2025

		NG Firewall JT 2025 - Órgãos Participantes																					
		TST		TRT1		TRT3		TRT4		TRT5		TRT6		TRT7		TRT9		TRT10		TRT11		TRT12	
Item	Descrição	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	
1	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico (...) - Tipo I - Pagamento em parcela única, antecipada.			1	1	1	1			1	1	1	2	1	1					1	1		
2	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico (...) - Tipo II - Pagamento em parcela única, antecipada.							1	1							1	1	1	2			1	1
3	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico (...) - Tipo III - Pagamento em parcela única, antecipada.																						
4	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico (...) - Tipo I - Pagamento em 5 parcelas fixas anuais.																						
5	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico (...) - Tipo III - Pagamento em 5 parcelas fixas anuais.																						
6	Aquisição de Cluster (...) - Tipo IV - Pagamento em parcela única, antecipada.	1	1																				
7	Aquisição de Cluster(...) - Tipo V - Pagamento em parcela única, antecipada.							1	1					1	1			1	2				
8	Voucher de Treinamento para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall	5	10	1	5	1	1	2	6	1	10	2	4	1	3	1	4	2	5	5	10	1	6
9	Licenciamento de Serviço de SD-WAN compatível com os equipamentos NGFW dos itens 1, 4 e 6 - Firewalls Tipo I e Tipo IV									1	1			1	1					1	1		
10	Licenciamento de Serviço de SD-WAN compatível com os equipamentos NGFW dos itens 2, e 7 - Firewalls Tipo II e Tipo V															1	1	1	2				

ANDERSON BASTOS 28/08/2025 18:21
ALEX WAGNER ZOLET 28/08/2025 18:34
PAULO SELEME CORREA 28/08/2025 18:49

		NG Firewall JT 2025 - Órgãos Participantes																					
		TST		TRT1		TRT3		TRT4		TRT5		TRT6		TRT7		TRT9		TRT10		TRT11		TRT12	
Item	Descrição	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max
11	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) (...) - Tipo VI									1	3					1	14						
12	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) (...) - Tipo VII									1	9			1	4	1	40			15	15		
13	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) (...) - Tipo VIII									1	21			1	15	1	10	1	18				
14	Licença de uso de solução de SASE e ZTNA por usuário pelo período de 60 meses			200	200			200	700	200	5600	200	400	200	1500	200	500	200	2500	500	1200	200	2500
15	Voucher de Treinamento para solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Access)			1	5			1	5	1	10	1	4	1	10	1	7	2	5	7	10	1	6
16	Serviço gerenciado mensal (...) por Cluster de equipamentos do Grupo I (itens 1, 4 e 6) - Tipo I e Tipo IV			1	1					1	1	1	2	1	1					1	1		
17	Serviço gerenciado mensa(...) por Cluster de equipamentos do Grupo I (itens 2 e 7) - Tipo II e Tipo V							1	2					1	1	1	1	1	2			1	1
18	Serviço gerenciado mensal (...) por Cluster de equipamentos do Grupo I (itens 3 e 5) - Tipo III																						
19	Serviço gerenciado mensal (...) por equipamentos do Grupo II (itens 11, 12 e 13) - Tipo VI, Tipo VII e Tipo VIII									1	33			1	15			1	18	15	15		

		NG Firewall JT 2025 - Órgãos Participantes																					
		TRT13		TRT14		TRT15		TRT16		TRT17		TRT18		TRT19		TRT20		TRT21		TRT22		TRT23	
Item	**Descrição**	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max
1	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico (...) - Tipo I - Pagamento em parcela única, antecipada.	1	1			1	1									1	1	1	1				
2	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico (...) - Tipo II - Pagamento em parcela única, antecipada.											1	1										
3	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico (...) - Tipo III - Pagamento em parcela única, antecipada.			1	1					1	1			1	1							1	1
4	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico (...) - Tipo I - Pagamento em 5 parcelas fixas anuais.							1	1														
5	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico (...) - Tipo III - Pagamento em 5 parcelas fixas anuais.																			1	1		
6	Aquisição de Cluster (...) - Tipo IV - Pagamento em parcela única, antecipada.																						
7	Aquisição de Cluster(...) - Tipo V - Pagamento em parcela única, antecipada.																						
8	Voucher de Treinamento para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall	6	6			1	2	1	5	1	2	1	7	1	3	2	4	2	2	1	5	1	3
9	Licenciamento de Serviço de SD-WAN compatível com os equipamentos NGFW dos itens 1, 4 e 6 - Firewalls Tipo I e Tipo IV																						
10	Licenciamento de Serviço de SD-WAN compatível com os equipamentos NGFW dos																						

		NG Firewall JT 2025 - Órgãos Participantes																					
		TRT13		TRT14		TRT15		TRT16		TRT17		TRT18		TRT19		TRT20		TRT21		TRT22		TRT23	
Item	Descrição	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max
	itens 2, e 7 - Firewalls Tipo II e Tipo V																						
11	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) (...) - Tipo VI																						
12	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) (...) - Tipo VII																						
13	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) (...) - Tipo VIII																						
14	Licença de uso de solução de SASE e ZTNA por usuário pelo período de 60 meses	200	2000	200	1000	200	4500	200	1000			200	2300	200	200	200	400	200	1700				
15	Voucher de Treinamento para solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Access)	6	6	1	4	2	15	1	10			1	7	1	5	2	4	3	7				
16	Serviço gerenciado mensal (...) por Cluster de equipamentos do Grupo I (itens 1, 4 e 6) - Tipo I e Tipo IV					1	1	1	1							1	1	1	1				
17	Serviço gerenciado mensa(...) por Cluster de equipamentos do Grupo I (itens 2 e 7) - Tipo II e Tipo V											1	1										
18	Serviço gerenciado mensal (...) por Cluster de equipamentos do Grupo I (itens 3 e 5) - Tipo III			1	1					1	1			1	1					1	1		
19	Serviço gerenciado mensal (...) por equipamentos do Grupo II (itens 11, 12 e 13) - Tipo VI, Tipo VII e Tipo VIII																						

Anexo III - Endereços de Entrega/Prestação dos Serviços

ANDERSON BASTOS
28/08/2025 18:21

ALEX WAGNER ZOLET
28/08/2025 18:34

PAULO SELEME CORREA
28/08/2025 18:50

Nome do órgão:	TST - Tribunal Superior do Trabalho
UG/UASG:	80001
CNPJ:	00.509.968/0001-48
Unidade responsável pela fiscalização:	CITEC - Coordenadoria de Infraestrutura Tecnológica
Servidor responsável:	Leonardo Lobo Pulceneli
Telefone:	(61) 3043-4474
E-mail:	leonardo.oulcineli@tst.jus.br
Endereço da prestação dos serviços/ entrega dos equipamentos:	Tribunal Superior do Trabalho Setor de Administração Federal Sul - SAFS Quadra 08, Conjunto A - CEP: 70.070-943 Bloco A, Sala A2.33

Nome do órgão:	Tribunal Regional do Trabalho da 1ª Região
UG/UASG:	80009
CNPJ:	02.578.421/0001-20
Unidade responsável pela fiscalização:	Divisão de Monitoramento e Prevenção de Incidentes de Segurança de TIC - DPSEG
Servidor responsável:	Francisco Assis de Paiva Dreyfuss
Telefone:	(21) 2380-7349/ 7282
E-mail:	dpseg@trt1.jus.br

Endereço da prestação dos serviços/ entrega dos equipamentos:	Av. Presidente Antônio Carlos, 251 12o andar Centro - Rio de Janeiro/RJ - CEP: 20.021-010

Nome do órgão:	Tribunal Regional do Trabalho da 3ª Região
UG/UASG:	080008
CNPJ:	01.298.583/0001-41
Unidade responsável pela fiscalização:	Secretaria de Infraestrutura Tecnológica
Servidor responsável:	Marden Pacheco Oliveira Diniz
Telefone:	(31) 3238-7908
E-mail:	marden@trt3.jus.br
Endereço da prestação dos serviços/ entrega dos equipamentos:	Rua Mato Grosso, 400 - Barro Preto - BH - MG

Nome do órgão:	Tribunal Regional do Trabalho da 4ª Região
UG/UASG:	080014
CNPJ:	02.520.619/0001-52
Unidade responsável pela fiscalização:	Coordenadoria de Segurança da Informação e Proteção de Dados
Servidor responsável:	Lucas Pozatti

Telefone:	(51) 3255-2784
E-mail:	lucas.pozatti@trt4.jus.br setic.csipd@trt4.jus.br
Endereço da prestação dos serviços/ entrega dos equipamentos:	Av. Praia de Belas, 1100, Prédio Anexo Administrativo, 2o andar - ala sul.

Nome do órgão:	Tribunal Regional do Trabalho da 5ª Região
UG/UASG:	080007
CNPJ:	02.839.639/0001-90
Unidade responsável pela fiscalização:	Divisão de Segurança Cibernética
Servidor responsável:	Ruth Marques Gomes de Oliveira
Telefone:	(71) 3319-7676
E-mail:	ruth.oliveira@trt5.jus.br
Endereço da prestação dos serviços/ entrega dos equipamentos:	Fórum 2 de Julho - Rua Ivonne Silveira, 248, Torre 2 - 2º andar, Paralela, Salvador - BA, 41.192-007.

Nome do órgão:	Tribunal Regional do Trabalho da 6ª Região
UG/UASG:	080006
CNPJ:	02.566.224/0001-90

Unidade responsável pela fiscalização:	Seção de Gestão de Redes de Computadores
Servidor responsável:	Igor Marcel Leal de Morais
Telefone:	(81) 99147-7505
E-mail:	igor.morais@trt6.jus.br redes@trt6.jus.br
Endereço da prestação dos serviços/ entrega dos equipamentos:	Rua Professor Augusto Wanderley Filho, 1-79 - Afogados, Recife - PE, 50770-290

Nome do órgão:	Tribunal Regional do Trabalho da 7ª Região
UG/UASG:	80004
CNPJ:	03.235.270/0001-70
Unidade responsável pela fiscalização:	Coordenadoria de Infraestrutura de TIC
Servidor responsável:	Robson Teixeira da Silva
Telefone:	(85) 2018-1942
E-mail:	robson.teixeira@trt7.jus.br
Endereço da prestação dos serviços/ entrega dos equipamentos:	Rua Desembargador Leite Albuquerque, 1077 – Anexo I – 3o andar – Aldeota – Fortaleza/CE – CEP 60.150-150

Nome do órgão:	Tribunal Regional do Trabalho da 9ª Região

UG/UASG:	80012
CNPJ:	03.141.166/0001-16
Unidade responsável pela fiscalização:	Secretaria de Infraestrutura e Operações (SIOP)
Servidor responsável:	Alexandre Tetsuo Yamauchi
Telefone:	(41) 3310-7100
E-mail:	sti@trt9.jus.br / alexandreyamauchi@trt9.jus.br
Endereço da prestação dos serviços/ entrega dos equipamentos:	Alameda Doutor Carlos de Carvalho, 528 – Centro - CEP: 80420-010 –Curitiba/ PR

Nome do órgão:	Tribunal Regional do Trabalho da 10ª Região
UG/UASG:	080016
CNPJ:	02.011.574/0001-90
Unidade responsável pela fiscalização:	Divisão de Segurança Cibernética
Servidor responsável:	Francisco Rogério Cavalcante da Ponte Filho
Telefone:	(61) 3348-1202
E-mail:	disec@trt10.jus.br
Endereço da prestação dos serviços/ entrega dos equipamentos:	Tribunal Regional do Trabalho da 10a Região SAS Quadra 1, Bloco "D" Praça dos Tribunais Superiores - Brasília/DF CEP: 70097-900

Nome do órgão:	Tribunal Regional do Trabalho da 11ª Região
UG/UASG:	80002
CNPJ:	01.671.187/0001-18
Unidade responsável pela fiscalização:	Secretaria de Tecnologia da Informação e Comunicação – SETIC
Servidor responsável:	Jean Ricardo de Oliveira Rebouças
Telefone:	(92) 3621-7474 / 7482
E-mail:	ti.seguranca@trt11.jus.br
Endereço da prestação dos serviços/ entrega dos equipamentos:	Av. Tefé, 930. Bairro: Praça 14 de Janeiro, Manaus/AM, CEP 69.020-090. Prédio Administrativo, 3º andar. Setor: Secretaria de Tecnologia da Informação e Comunicações / Seção de Manutenção de Bens de TIC

Nome do órgão:	Tribunal Regional do Trabalho da 12ª Região
UG/UASG:	080013
CNPJ:	02.482.005/0001-23
Unidade responsável pela fiscalização:	Coordenadoria de Segurança de TIC
Servidor responsável:	Anderson Bastos
Telefone:	(48) 3216-4125
E-mail:	anderson.bastos@trt12.jus.br
Endereço da prestação dos serviços/ entrega dos	Rua Esteves Júnior, 395, Centro - Florianópolis/SC CEP 88015-905

equipamentos:	

Nome do órgão:	Tribunal Regional do Trabalho da 13ª Região
UG/UASG:	080005
CNPJ:	02.658.544/0001-70
Unidade responsável pela fiscalização:	Secretaria de Tecnologia da Informação e Comunicação (SETIC)
Servidor responsável:	Ricardo José de Medeiros II
Telefone:	(83) 3533-6173
E-mail:	seguranca-ti@trt13.jus.br
Endereço da prestação dos serviços/ entrega dos equipamentos:	Av. Corálio Soares de Oliveira, S/N, Centro, João Pessoa/PB, CEP 58.013-260.

Nome do órgão:	Tribunal Regional do Trabalho da 14ª Região
UG/UASG:	80015
CNPJ:	03.326.8015/0001-53
Unidade responsável pela fiscalização:	Divisão de Segurança da Informação
Servidor responsável:	Wainner Brum Caetano
Telefone:	(69) 3218-6315
E-mail:	wainner.caetano@trt14.jus.br

	setic@trt14.jus.br
Endereço da prestação dos serviços/ entrega dos equipamentos:	Rua Almirante Barroso, n.o 600, Bairro Mocambo. Porto Velho-RO. CEP: 76.801-901

Nome do órgão:	Tribunal Regional do Trabalho da 15ª Região
UG/UASG:	080011
CNPJ:	03.773.524/0001-03
Unidade responsável pela fiscalização:	Secretaria de Tecnologia da Informação e Comunicação
Servidor responsável:	Herbert Wittmann
Telefone:	(19) 3231-9500 - ramal 2842
E-mail:	herbert@trt15.jus.br
Endereço da prestação dos serviços/ entrega dos equipamentos:	Rua Dr. Quirino, 1080 - Centro. CEP:13015-081 - Campinas/SP

Nome do órgão:	Tribunal Regional do Trabalho da 16ª Região
UG/UASG:	080018
CNPJ:	23.608.631/0001-93
Unidade responsável pela fiscalização:	Divisão de Infraestrutura e Segurança da Informação (DIVINFRA/SETIC)

Servidor responsável:	Rodrigo Silveira Alexandre
Telefone:	(98) 2109-9566
E-mail:	setic@trt16.jus.br / rodrigo.alexandre@trt16.jus.br
Endereço da prestação dos serviços/ entrega dos equipamentos:	Av. Senador Vitorino Freire, No 2001, Areinha, CEP: 65030-015, São Luís-MA

Nome do órgão:	Tribunal Regional do Trabalho da 17ª Região
UG/UASG:	80019
CNPJ:	02.488.507/0001-61
Unidade responsável pela fiscalização:	Secretaria de Tecnologia da Informação e Comunicação
Servidor responsável:	Fabbiano Fiorin Ferrari
Telefone:	(27) 3185-2032 (27) 3321-2515
E-mail:	setic@trt17.jus.br; coinf@trt17.jus.br
Endereço da prestação dos serviços/ entrega dos equipamentos:	SETIC - Secretaria de Tecnologia da Informação e Comunicação Avenida Nossa Senhora dos Navegantes, no 1245, Enseada do Suá, Vitória/ES, CEP 29.050-335.

Nome do órgão:	Tribunal Regional do Trabalho da 18ª Região
UG/UASG:	080020

CNPJ:	02.395.868/0001-63
Unidade responsável pela fiscalização:	Coordenadoria de Segurança da Informação
Servidor responsável:	Vinícius Graciano Elias
Telefone:	(62) 3222-5822
E-mail:	vinicius.elias@trt18.jus.br
Endereço da prestação dos serviços/ entrega dos equipamentos:	Av. T–1 esquina com a Rua T–51, Lotes 1 a 24, Qd. T–22, Setor Bueno, Goiânia–GO, CEP: 74215-901

Nome do órgão:	Tribunal Regional do Trabalho da 19ª Região
UG/UASG:	80022
CNPJ:	35.734.318/0001-80
Unidade responsável pela fiscalização:	SETIC / Divisão de Segurança da Informação e Proteção de Dados - DSIPD
Servidor responsável:	Leonardo Albuquerque de Rezende
Telefone:	(82) 2121-6280
E-mail:	leonardo.rezende@trt19.jus.br
Endereço da prestação dos serviços/ entrega dos equipamentos:	Av. da Paz, 2076 - Centro, Maceió - AL, 57020-440

Nome do órgão:	Tribunal Regional do Trabalho da 20ª Região
UG/UASG:	80023
CNPJ:	01.445.033/0001-08
Unidade responsável pela fiscalização:	Divisão de Segurança da Informação e Proteção de Dados
Servidor responsável:	Rozana Alves Farani Farias
Telefone:	(79) 2105-8712
E-mail:	diseg@trt20.jus.br
Endereço da prestação dos serviços/ entrega dos equipamentos:	Secretaria de Tecnologia da Informação e Comunicação Av. Carlos Rodrigues da Cruz, s/no - Capucho - CEP: 49081-015, Centro Administrativo Gov. Augusto Franco – Aracaju/ SE.

Nome do órgão:	Tribunal Regional do Trabalho da 21ª Região
UG/UASG:	080021
CNPJ:	02.544.593/0001-82
Unidade responsável pela fiscalização:	SETIC/SESEC
Servidor responsável:	Gilberto Coelho de Azevedo Neto
Telefone:	(84) 4006-3272
E-mail:	gilbertoneto@trt21.jus.br
Endereço da prestação dos serviços/ entrega dos equipamentos:	Av. Capitão-Mor Gouveia, 3104 - Lagoa Nova - Natal/RN CEP: 59063-900. Subsolo do prédio administrativo. Ponto de referência: Entrada pela Rua Lauro Pinto (ao lado da PF/RN)

Nome do órgão:	Tribunal Regional do Trabalho da 22ª Região
UG/UASG:	80024
CNPJ:	03.458.141/0001-40
Unidade responsável pela fiscalização:	Secretaria de Tecnologia da Informação e Comunicação - STIC
Servidor responsável:	Igor Coelho Marques de Sousa
Telefone:	(86) 99949-9669
E-mail:	igor.sousa@trt22.jus.br
Endereço da prestação dos serviços/ entrega dos equipamentos:	Rua João da Cruz Monteiro, 1694. Cristo Rei. Teresina - PI. CEP: 64.014-210

Nome do órgão:	Tribunal Regional do Trabalho da 23ª Região
UG/UASG:	80025
CNPJ:	37.115.425/0001-56
Unidade responsável pela fiscalização:	Coordenadoria de Segurança da Informação e Proteção de Dados
Servidor responsável:	Leandro Cesar Pereira Miranda
Telefone:	(65) 3648-4026
E-mail:	csi@trt23.jus.br
Endereço da	Avenida Historiador Rubens de Mendonça, 3355, Centro Político

prestação dos serviços/ entrega dos equipamentos:	e Administrativo, Cuiabá/MT, CEP 78049-935