PREFEITURA MUNICIPAL DA ESTÂNCIA TURÍSTICA DE PARAGUAÇU PAULISTA

Departamento de Tecnologia da Informação

Estudo Técnico Preliminar 005/25

INTRODUÇÃO

O Estudo Técnico Preliminar – ETP tem por objetivo identificar e analisar os cenários para o atendimento a demanda da Administração Municipal de contratar uma nova solução de firewall de próxima geração (Next-Generation Firewall – NGFW, em inglês), bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

O presente estudo técnico foi elaborado com base no artigo 6º, inciso XX, combinado com § 1º e 2º, da Lei 14.133/21, Decreto Municipal nº 7.055, de 18 de março de 2023, art. 15.

DESCRIÇÃO DO OBJETO E DA NECESSIDADE DA CONTRATAÇÃO, CONSIDERANDO O PROBLEMA A SER RESOLVIDO SOB A PERSPECTIVA DO INTERESSE PÚBLICO.

1. Descrição do Objeto

Contratação de empresa especializada para fornecimento, implantação, configuração e suporte técnico de solução de segurança de rede do tipo Firewall de Próxima Geração (Next Generation Firewall – NGFW), composta por appliance físico dedicado, licenciamento de software, e serviços associados especificações e quantidades descritas no item 9, como serviço.

A solução deverá contemplar:

- Appliance físico dedicado com capacidade mínima de throughput de prevenção de ameaças de 10 Gbps, com suporte a alta disponibilidade (HA) e redundância de fontes;
- Licenciamento completo por [ex. 36 meses], incluindo funcionalidades de:
- Firewall de inspeção profunda (camada 7);
- IPS/IDS (sistema de prevenção/detecção de intrusos);
- Antivírus e antimalware;
- Filtro de conteúdo web;
- Controle de aplicações e usuários;
- VPN (IPSec e SSL);
- Proteção contra ameaças avançadas (ATP);
- Console de gerenciamento centralizado, com interface web intuitiva e geração de relatórios e logs;
- Serviços de instalação, configuração e ativação, com repasse de conhecimento técnico para equipe interna;
- Suporte técnico especializado durante o período de vigência contratual, com SLA definido;
- Garantia de hardware e atualizações de software durante todo o período contratual;

2. Justificativa e Objeto da Contratação

2.1. A presente contratação está prevista no orçamento do Plano de Contratação Anual (PCA), exercício de 2025 que consta para consulta no Portal da Transparência no site www.eparguacu.sp.gov.br, ou no link http://sistemas2.eparaguacu.sp.gov.br:8079/transparencia, conforme item 5868;

No cenário atual da Administração Municipal, as atividades administrativas são amparadas fortemente no uso de soluções de TI – equipamentos, softwares e sistemas da informação – que se tornaram vitais para o funcionamento e melhoria dos serviços prestados aos cidadãos. Como consequência, a proteção do ambiente tornou-se fator essencial para manutenção da disponibilidade, confidencialidade e integridade dos serviços de TI e do funcionamento da Administração Municipal, bem como para manutenção da confidencialidade, integridade, disponibilidade e autenticidade dos dados.

Por conseguinte, a expansão da utilização da Internet com a interconexão de instituições, corporações e pessoas, e o tráfego imenso de informação na rede provocou o interesse de pessoas mal-intencionadas visando à obtenção de vantagens financeiras, coleta de informações confidenciais, prática de vandalismo e golpes, realização de ataques ou a mera disseminação de mensagens indesejadas ou informações falsas.

As formas de ataque, especialmente os vindos da internet, tornam-se cada vez mais sofisticadas e a cada dia novos tipos de ataques são desenvolvidos e novas vulnerabilidades são exploradas. É importante, portanto, implementar métodos de segurança que possam

auxiliar na tentativa de proteção dos dados e a segurança da informação de forma dinâmica.

Vale ressaltar que um bom método de segurança é garantir que os recursos tecnológicos de segurança estejam bem alocados dentro da infraestrutura e que estejam funcionando a contento. Não obstante, a busca por redução de complexidade nos itens supracitados se torne cada vez mais necessária devido à grande quantidade de ferramentas e serviços disponibilizados pelas soluções de segurança. Além disso, também é interessante buscar a facilidade da gerência da solução. Uma arquitetura robusta, porém, mais simplificada, auxilia na disponibilidade de todos os serviços prestados.

3. Requisitos Necessários para a Contratação.

3.1. Fornecer os objetos de acordo com as especificações e quantitativos em conformidade com as condições deste instrumento, obrigando-se a substitui aquele(s) não achado(s) conforme(s) pela contratante;
3.2. Responder, integralmente, por perdas e danos que vier a causar a esta Prefeitura ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou dos seus prepostos, independentemente de outras cominações contratuais ou legais a que estiver sujeita;
3.3. Fornecer o(s) serviço(s) e adotar todas medidas preventivas no sentido de se minimizar acidentes ou danos que venham a comprometer a qualidade do(s) serviço(s) fornecido(s);
3.4. Manter, pessoal e equipamentos suficientes para o atendimento;
3.5. Assumir a inteira responsabilidade quanto à qualidade do fornecimento;
3.6. Fornecer o objeto obedecendo às quantidades requisitadas, qualidade, horários, prazos e locais estabelecidos para a prestação dos serviços;
3.7. Cumprir todos os requisitos do item 9 (nove) deste Estudo Técnico Preliminar;
3.8. Cumprir todas as demais cláusulas do contrato;

4. Estimativa das Quantidades, Acompanhadas das Memórias de Cálculo e dos Documentos que lhe dão Suporte

4.1. As quantidades de bens e serviços necessários estimados encontram-se abaixo:

Lote	Item	Descrição/Especificação	Unidade de Medida	Quant.
01	01	Contratação de empresa especializada para fornecimento, implantação, configuração e suporte técnico de solução de segurança de rede do tipo Firewall de Próxima Geração (Next Generation Firewall – NGFW), composta por appliance físico dedicado, licenciamento de software, e serviços associados especificações e quantidades descritas no item 9, como serviço.	Mês	60

4.2. O quantitativo da aquisição dos itens, foram estimados com base em contrato vigente, acrescidos de uma estimativa de demanda de 20%, visto que o contrato pode perdurar por até 10 anos;

5. Levantamento de Mercado – Analise das Alternativas Existentes

Com base neste levantamento, cenários ou arranjos poderão ser formados para compor as soluções possíveis para atendimento da necessidade

5.1. Identificação das Soluções:

Solução	Descrição da Solução
1	Soluções baseadas exclusivamente em software open source
2	Solução oferecida como serviço
3	Aquisição de solução proprietária

5.2. Análise Comparativa Técnica de Soluções:

•Solução 1: Software Open Source

Solução em software livre, são um tipo de software onde o código-fonte está disponível para todos que quiserem usar. Ele é construído, assim como sua manutenção, de maneira colaborativa. Dessa forma, qualquer pessoa pode investigar, alterar e redistribuí-lo. O Open Source beneficia diferentes iniciativas, pois não está focado em obter lucros relacionados à propriedade intelectual.

São soluções que costumam não ter custos com licenças ou relacionados a propriedade intelectual, logo em termos financeiros, costumam ter seu custo reduzido ao comparar com uma solução proprietária. Destaca-se que empresas podem utilizá-los como base para comerciar um produto, cobrando por subscrições de atualizações de bases, correções etc.

São disponibilizados no formato de software, sendo agnósticos a qualquer tipo de hardware;

Por terem seu código-fonte livre, é possível que seja realizada diversas customizações no software par atender requisitos específicos da instituição;

Dependendo da aplicação, é possível contar com o auxílio de outros desenvolvedores e de uma comunidade voltada para aquela ferramenta;

•Solução 2: Proprietária como Serviço

A utilização de contratação de serviço de locação, é uma modalidade a qual a empresa realiza uma assinatura, com pagamento mensal ou anual.

Assim, não há responsabilidade técnica por parte da equipe interna pois todas as funções relacionadas ao suporte técnico, manutenção e aquisição de equipamentos ficam a cargo da empresa contratada.

A contratada realiza todas as atividades técnicas como configuração, manutenção, backup, melhorias e resolução de problemas.

Esse tipo de serviço por ser adquirido em diversas formas a fim de atender as demandas da contratante.

Geralmente, há uma equipe totalmente especializada no assunto para operar a solução e realizar um atendimento satisfatório. Esse atendimento pode ser tanto em dias comerciais, como na modalidade 24x5x365 ou 24x7x365;

A contratante também não precisa se preocupar em aquisição de equipamentos para substituição ou treinamentos regulares para equipe interna.

•Solução 3: Proprietário

Solução proprietária é aquela à qual é desenvolvida por uma empresa a qual detém o direito sobre aquele conjunto de ferramentas.

Para ter acesso de uso, de forma legal, é necessário comprar a licença ou subscrição.

Esse tipo de solução geralmente conta com o apoio e suporte do fabricante em casos de ajuda, bugs ou outras necessidades. São ferramentas que são conhecidas pelo mercado e há uma boa oferta de profissionais que entendem e dão suporte ou treinamento mediante a um contrato de serviço.

Nessa modalidade, a equipe interna de uma empresa pode passar por um treinamento fornecido pela fabricante ou um terceiro homologado.

Geralmente são ofertados em forma de appliance físico ou virtual. Em ambos os casos, a contratante terá algum nível de suporte da fabricante durante o período que a licença estiver ativa.

É usual que esse tipo de solução seja utilizado por empresas de porte grande devido a ter um respaldo direto do fabricante e um elevado investimento.

6. Registro de Soluções Consideradas Inviáveis

Inicialmente, temos que levar em consideração a figura abaixo a qual auxiliou a equipe técnica para desenhar a arquitetura.

O “quadrante mágico” demonstra quais são os melhores firewalls de mercado atualmente.

O quadrante é lido da seguinte maneira, sendo do melhor para o menos hábil: Lideres, Desafiantes, Empresas de Nichos e Visionários.

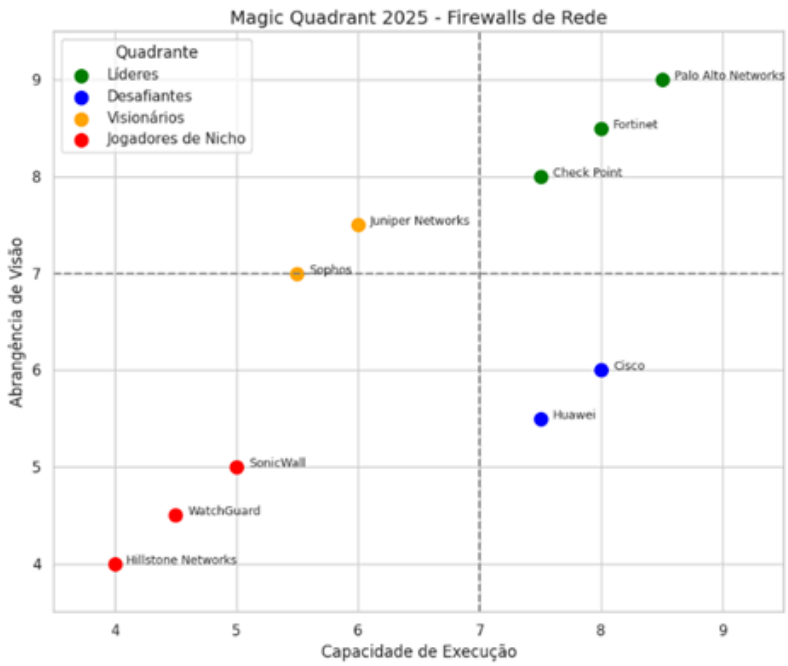

Figura 1 – Quadrante Mágico para Firewalls NGFW

•Solução Inviável: Solução baseadas exclusivamente em software open source (solução 1).

Não foram consideradas uma vez que (a) necessitem de investimento em infraestrutura (aquisição de equipamentos, sistemas operacionais etc.) (b) exigem também, no caso de software pago, a manutenção de contratos de subscrição para atualização de software e das bibliotecas de assinatura de código malicioso, quando contemplam esta funcionalidade, (c) exigem, no caso de software livre, a designação de equipe de segurança dedicada e especializada e investimentos em processos contínuos de capacitação, (d) impõem restrições à alta disponibilidade e à prestação de suporte adequado e tempestivo, além de (e) não implementarem todos os requisitos de segurança de porte corporativo, de forma ampla e efetiva.

Por sua vez, também não foram encontradas soluções de firewall que estivesse nos dois primeiros quadrantes do Gartner.

- Solução Inviável: Solução oferecida como proprietária (Solução 3).

Não foram consideradas, pois promovem o dispêndio de recursos financeiros elevados, para a compra do equipamento mais as ativações de licença de uso, custos com atualizações tecnológicas, e também a obsolescência tecnológica, comum em soluções adquiridas e mantidas internamente.

7. Da solução Escolhida

7.1. Dentre as soluções passíveis de atendimento as necessidades levantadas, optamos pela constante na Solução nº 02, considerando as seguintes motivações:

7.1.1. O cenário apresentado na solução 02, preza pela manutenção do modelo atualmente contratado e que inclusive é o mesmo adotado pelos diversos órgãos da estrutura administrativa municipal, estadual e federal;

7.1.2. A contratação de solução proprietário como serviço (locação), torna-se mais viável, tanto no impacto financeiro quando na atualização tecnológica;

8. Estimativa de Preço da Contratação

8.1. **Fundamentação:** Estimativa do valor da contratação, acompanhada dos preços unitários referenciais, das memórias de cálculo e dos documentos que lhe dão suporte, que poderão constar de anexo classificado, se a administração optar por preservar o seu sigilo até a conclusão da licitação (Inciso VI § 1º da Lei 14.133/2021 e art. 7º, inciso VI da IN 040/2010);

8.2. A presente contratação tem valor estimado em R$ 615.822,00 (Seiscentos e quinze mil, oitocentos e vinte e dois reais) conforme mapa de apuração de preços da cesta nº 86671, anexo a este, obtido através do site app.sgmstecnologia.com.br;

9. Descrição da Solução Como Um Todo

9.1. Características de Hardware

9.1.1. Deve suportar, no mínimo, 10 (dez) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente de tamanho de pacote;

9.1.2. Deve suportar, no mínimo, 3 (três) milhões de conexões simultâneas;

9.1.3. Deve suportar, no mínimo, 250.000 (duzentos e cinquenta mil) novas conexões por segundo;

9.1.4. Deve suportar, no mínimo, 12 (doze) Gbps de throughput VPN IPSec;

9.1.5. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 2.000 (dois mil) túneis de VPN IPSec Site-to-Site simultâneos;

9.1.6. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 5.000 (cinco mil) túneis de clientes VPN IPSec simultâneos;

9.1.7. Deve suportar, no mínimo, 02 (dois) Gbps de throughput de VPN SSL;

9.1.8. Deve suportar, no mínimo, 500 (quinhentos) clientes de VPN SSL simultâneos;

9.1.9. Deve suportar, no mínimo, 05 (cinco) Gbps de throughput de IPS;

9.1.10. Deve suportar, no mínimo, 04 (quatro) Gbps de throughput de Inspeção SSL;

9.1.11. Deve suportar, no mínimo, 03 (três) Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS e AntiMalware.

9.1.12. Deve possuir, pelo menos, 16 (dezesseis) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;

9.1.13. Deve possuir, pelo menos, 8 (oito) interfaces Gigabit Ethernet com conectores SFP;

9.1.14. Deve possuir, pelo menos, 4 (quatro) interfaces 10 Gigabit Ethernet com conectores SFP+;

9.1.15. Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para gerenciamento;

9.1.16. Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para Alta-Disponibilidade;

9.1.17. Deve possuir unidade do tipo SSD com no mínimo 480 GB para armazenamento de informações locais;

9.1.18. Deve estar licenciado para gerenciar até 120 (cento e vinte) pontos de acesso sem fio e 60 (sessenta) switches simultaneamente em um único appliance;

9.1.19. Deve possuir fonte de alimentação AC redundante;

9.1.20. Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliance;

9.2. Características Gerais para Firewalls de Próxima Geração

9.2.1. A solução deve consistir em plataforma de proteção e balanceamento inteligente de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), console de gerência e monitoração.

9.2.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

9.2.3. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

9.2.4. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;

9.2.5. As funcionalidades de proteção de rede que compõe a solução de segurança, podem funcionar em múltiplos appliances desde que atendam a todos os requisitos desta especificação;

9.2.6. Deverá possuir e estar licenciado pelo período de 36 (trinta e seis) meses com as seguintes funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec,

Controle de Aplicações, Prevenção de Perda de Dados (DLP) e Virtualização.

9.3. Funcionalidades de Rede e Firewall

9.3.1. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
9.3.2. Os dispositivos de proteção de rede devem possuir suporte a Vlans;
9.3.3. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
9.3.4. Os dispositivos de proteção de rede devem possuir suporte a DHCP Cliente, Server e Relay;
9.3.5. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
9.3.6. Deve possuir a funcionalidade de tradução de endereços estáticos- NAT (Network Address Translation), um para um (1-to-1), N-para-um (N-to-1), vários para um, NAT64, NAT66, NAT46 e PAT;
9.3.7. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
9.3.8. Deverá suportar sFlow ou Netflow;
9.3.9. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;
9.3.10. Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;
9.3.11. Deve suportar o protocolo padrão da indústria VXLAN;
9.3.12. Deve implementar o protocolo ECMP;
9.3.13. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;
9.3.14. Enviar log para sistemas de monitoração externos;
9.3.15. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;
9.3.16. Deve possui mecanismos de proteção anti-spoofing;
9.3.17. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP4 e OSPFv2);
9.3.18. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
9.3.19. Suportar OSPF graceful restart;
9.3.20. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
9.3.21. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
9.3.22. Deve suportar Modo Camada- 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
9.3.23. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;
9.3.24. A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs e Tabelas FIB;
9.3.25. Deverá possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;
9.3.26. O modo de Alta-Disponibilidade (HA) deve possibilitar monitoração de falha de link;
9.3.27. A solução deve suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática;
9.3.28. A solução deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI, Cisco ACI e Kubernetes;
9.3.29. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;
9.3.30. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;
9.3.31. Deverá suportar controle por zonas de segurança;
9.3.32. Deverá suportar controles de políticas por porta e protocolo;
9.3.33. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;
9.3.34. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
9.3.35. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);
9.3.36. Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);
9.3.37. Deve decriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;
9.3.38. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;
9.3.39. Suporte a objetos e regras IPV6;
9.3.40. Suporte a objetos e regras multicast;
9.3.41. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

9.4. Funcionalidades de Controle de Aplicações

9.4.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
9.4.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
9.4.3. Reconhecer pelo menos 4.000 (quatro 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;
9.4.4. Deverá possuir, pelo menos, 15 (quinze) categorias para classificação de aplicações;
9.4.5. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared,

dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

9.4.6. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

9.4.7. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;

9.4.8. Para tráfego criptografado SSL, deve decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

9.4.9. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação;

9.4.10. Identificar o uso de táticas evasivas via comunicações criptografadas;

9.4.11. Atualizar a base de assinaturas de aplicações automaticamente;

9.4.12. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

9.4.13. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

9.4.14. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

9.4.15. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;

9.4.16. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

9.4.17. Deve alertar o usuário quando uma aplicação for bloqueada;

9.4.18. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;

9.4.19. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;

9.4.20. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;

9.4.21. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);

9.4.22. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, fabricante e popularidade;

9.4.23. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;

9.4.24. Deve permitir forçar o uso de portas específicas para determinadas aplicações;

9.5. Funcionalidade de Prevenção de Intrusão e Ameaças

9.5.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

9.5.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

9.5.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

9.5.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;

9.5.5. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

9.5.6. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

9.5.7. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

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

9.5.9. Deve permitir o bloqueio de vulnerabilidades;

9.5.10. Deve permitir o bloqueio de exploits conhecidos;

9.5.11. Deve incluir proteção contra-ataques de negação de serviços;

9.5.12. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;

9.5.13. Detectar e bloquear a origem de portscans;

9.5.14. Bloquear ataques efetuados por worms conhecidos;

9.5.15. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

9.5.16. Possuir assinaturas para bloqueio de ataques de buffer overflow;

9.5.17. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

9.5.18. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

9.5.19. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB/CIFS, SMTP e POP3;

9.5.20. Identificar e bloquear comunicação com botnets;

9.5.21. Registrar no console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

9.5.22. Os eventos devem identificar o país de onde partiu a ameaça;

9.5.23. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

9.5.24. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

9.5.25. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.
9.5.26. A solução deve ter capacidade de enviar artefatos suspeitos para serem executados em ambiente controlado na nuvem do fabricante
9.5.27. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
9.5.28. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;

9.6. Funcionalidade de Filtro de Conteúdo WEB e DNS
9.6.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
9.6.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;
9.6.3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;
9.6.4. Deve permitir que os usuários sejam identificados através de consulta em uma base do Active Directory, permitindo que sua autenticação no domínio, não seja solicitada novamente para navegar através da solução;
9.6.5. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
9.6.6. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
9.6.7. Possuir pelo menos 80 (oitenta) categorias de URLs;
9.6.8. Deve possuir a função de exclusão de URLs do bloqueio;
9.6.9. Permitir a customização de página de bloqueio;
9.6.10. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;
9.6.11. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos e Comando e Controle (C&C) de botnets conhecidas;
9.6.12. Deve possuir filtro de domínio DNS baseado em categorias para inspecionar o tráfego DNS com classificação de domínios continuamente atualizado;

9.7. Funcionalidade de Identificação de Usuários
9.7.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, eDirectory e base de dados local;
9.7.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
9.7.3. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior;
9.7.4. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;
9.7.5. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
9.7.6. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
9.7.7. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
9.7.8. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
9.7.9. Deve suportar o envio e recebimento de credenciais via RADIUS;
9.7.10. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

9.8. Funcionalidade de Filtro de Dados
9.8.1. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP);
9.8.2. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
9.8.3. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
9.8.4. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

9.9. Funcionalidade de Geolocalização
9.9.1. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;
9.9.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
9.9.3.
9.9.4. FUNCIONALIDADE DE VPN

9.9.5. Suportar VPN Site-to-Site e Client-To-Site;
9.9.6. Suportar IPSec VPN;
9.9.7. A VPN IPSEc deve suportar 3DES;
9.9.8. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;
9.9.9. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
9.9.10. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
9.9.11. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
9.9.12. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI
9.9.13. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
9.9.14. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
9.9.15. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;
9.9.16. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
9.9.17. Atribuição de DNS nos clientes remotos de VPN;
9.9.18. Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, AntiSpyware e filtro de URL para tráfego dos clientes remotos conectados na VPN;
9.9.19. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
9.9.20. Suportar leitura e verificação de CRL (Certificate Revocation List);
9.9.21. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis VPN;
9.9.22. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Após autenticação do usuário na estação;
9.9.23. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Sob demanda do usuário;
9.9.24. Deverá manter uma conexão segura com o portal durante a sessão;
9.9.25. O agente de VPN client-to-site deve ser compatível com pelo menos: Windows (10 ou superior), Ubuntu Linux (22.04 ou superior), Red Hat Linux (7.4 ou superior), CentOS Stream (9 ou superior), Fedora Linux (36 ou superior) e macOS (v13 ou superior);

9.10. Funcionalidade de QOS, traffic Shaping e Priorização de Tráfego

9.10.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube e redes sociais, etc.) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;
9.10.2. Suportar a criação de políticas de QoS e Traffic Shaping para os seguintes itens:
9.10.3. Endereço de origem;
9.10.4. Endereço de destino;
9.10.5. Usuário e grupo;
9.10.6. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
9.10.7. Por porta;
9.10.8. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;
9.10.9. O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como YouTube, Facebook, entre outros;
9.10.10. O QoS deve possibilitar a definição de fila de prioridade;
9.10.11. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;
9.10.12. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
9.10.13. Suportar modificação de valores DSCP para o Diffserv;
9.10.14. Suportar priorização de tráfego usando informação de ToS (Type of Service);
9.10.15. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;
9.10.16. Deve suportar QOS (Traffic-Shapping), em interface agregadas ou redundantes;
9.10.17. Deve possibilitar a definição de bandas distintas para download e upload;

9.11. Funcionalidade de Balanceamento Inteligente de Links

9.11.1. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;
9.11.2. A solução deve ser capaz de agregar vários links em uma interface virtual;
9.11.3. A solução deve ser possível criar políticas de roteamento inteligente, mediante regras pré-estabelecidas considerando a verificação das seguintes condições: Endereços de origem, Grupos de usuários, Endereços de destino, Serviços na Internet e Aplicações de camada 7 (O365 Exchange, AWS, Dropbox e etc);
9.11.4. A solução deve ser capaz de medir o status de qualidade do link baseando-se em critérios mínimos de latência, jitter e perda de pacotes, onde deve ser possível configurar um valor limite para cada um destes itens que será utilizado como gatilho para fator de decisão nas regras de tráfego de saída e balanceamento inteligente;
9.11.5. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de balanceamento em condições em que a largura de banda é modificada;
9.11.6. A solução deve ser capaz de monitorar a qualidade e identificar falhas nos links, enviando sinais por meio de cada link para servidores ou aplicações, permitindo utilizar protocolos como Ping, HTTP, TCP ECHO, UDP ECHO, DNS, TCP Connect

e TWAMP (Two-way Active Measurement Protocol). Deve suportar ainda um método para mensurar a qualidade do tráfego de voz corporativo baseado em MOS (Mean Opinion Score);

9.11.7. A solução deve possibilitar balanceamento de tráfego entre conexões WAN, de forma em que o algoritmo de balanceamento de carga utilizado possa ser configurado considerando os seguintes parâmetros: Sessões, Volume de tráfego, IP de origem e destino e Transbordo de link (Spillover).

9.11.8. A solução deve possibilitar a criação de regras para seleção das interfaces e suas prioridades que serão utilizadas para encaminhar o tráfego de saída da rede, considerando os seguintes critérios:

9.11.9. Manual: Deve permitir que as interfaces tenham as prioridades atribuídas manualmente.

9.11.10. Melhor Qualidade: Deve permitir que as interfaces recebam uma prioridade com base na qualidade do link no qual a interface está conectada, considerando o monitoramento de um dos seguintes parâmetros com valores customizáveis: latência, jitter, perda de pacotes ou largura de banda;

9.11.11. Menor Custo: Deve permitir que as interfaces recebam uma prioridade com base no custo atribuído a interface, considerando a satisfação dos parâmetros de qualidade do link no qual a interface está conectada;

9.11.12. Balanceamento de Carga: Deve permitir que o tráfego seja distribuído entre todas as interfaces disponíveis com base em algoritmos de balanceamento de carga e satisfação dos parâmetros customizados de qualidade do link no qual a interface está conectada;

9.11.13. A solução de balanceamento inteligente deve suportar marcação de pacotes DSCP nas definições e regras para o tráfego balanceado;

9.11.14. A solução de balanceamento inteligente de links deve suportar Roteamento dinâmico (OSPFv2/v3, BGPv4/BGP4+);

9.11.15. A solução deve realizar o reconhecimento de aplicações, em camada 7, de pelo menos 3.000 (três mil) aplicações, incluindo Aplicações SaaS, em Nuvem e Multimídia (Vimeo, YouTube, Facebook, etc);

9.11.16. Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos;

9.11.17. A solução deve possibilitar a criação e uso de túneis VPN de forma dinâmica entre unidades remotas, para aplicações sensíveis. Uma vez que as unidades trocam informações entre si, o tráfego deve ser encaminhado diretamente entre as unidades remotas sem passar pela unidade Sede;

9.11.18. A solução deve permitir a duplicação de pacotes entre dois ou mais links, que atendam os parâmetros de qualidade estabelecidos, objetivando uma melhor experiência de uso de aplicações;

9.11.19. A solução deve possuir recurso para controlar e corrigir erros (FEC) na transmissão de dados, enviando dados redundantes através de túnel VPN em antecipação à perda de pacotes que pode ocorrer durante o trânsito;

9.11.20. A solução deve permitir a customização de intervalo de tempo em que é feita a verificação da situação de um link, assim como, permitir definir a quantidade de falhas encontradas no link antes de declará-lo inativo, com objetivo de identificar oscilações nos links, que possam impactar os serviços e a experiência dos usuários;

9.11.21. A solução deve suportar nativamente conectores com clouds públicas;

9.11.22. Deve possibilitar a definição de largura de banda distintas nas interfaces para download e upload;

9.11.23. A solução deve prover estatísticas em tempo real a respeito da utilização da largura de banda (upload e download) e nível de qualidade dos links (perda de pacote, jitter e latência);

9.11.24. Deve implementar balanceamento de link por hash do IP de origem;

9.11.25. Deve implementar balanceamento de link por hash do IP de origem e destino;

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

9.11.27. O appliance físico deve apresentar compatibilidade com modems USB (3G/4G), onde estes sejam capazes de funcionar como circuito ativo em relação à saída principal de Internet, e alternativamente funcionar como circuito Standby, onde apenas seja acionado na eventualidade de falha no link principal;

9.11.28. Deve ser possível extrair informações de desempenho das verificações de saúde mediante REST API, permitindo assim a consolidação de tais informações em alguma aplicação terceira.

9.12. Software de Gestão Centralizada e Armazenamento de Logs

9.12.1. Deverá ser entregue como appliance físico ou virtual em nuvem, compatível com rack 19” (polegadas) deverá possuir todos acessórios necessários para sua instalação;

9.12.2. Os softwares de gestão centralizada e armazenamento de logs poderão ser entregues em appliances separados, caso não seja possível entregar em um mesmo appliance;

9.12.3. O software deverá ser fornecido em sua versão mais atualizada;

9.12.4. Deverá possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos;

9.12.5. O gerenciamento da solução deverá possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;

9.12.6. O Software de Gestão Centralizada deverá ser homologado e totalmente compatível com o item “Firewall com Suporte, garantia e licenças de proteção com vigência de 60 meses” especificado neste Estudo Técnico Preliminar para permitir o gerenciamento dos equipamentos e o armazenamento de logs gerados pelos mesmos;

9.12.7. Deverá permitir o armazenamento de logs sem limite de tempo para retenção;

9.12.8. Deverá permitir o armazenamento de logs sem limite de tempo e reconhecer e/ou permitir alocar um tamanho de disco de no mínimo 1TB;

9.12.9. Deverá permitir armazenamento de no mínimo 15 GB de logs por mês;

9.12.10. Deverá permitir armazenamento de no mínimo 500 MB de logs por dia;

9.12.11. Deverá permitir a exportação dos logs para outros sistemas;

9.12.12. Deverá permitir controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções;

9.12.13. Deverá permitir controle global de políticas para todos os equipamentos que compõe a plataforma de segurança;

9.12.14. Deverá permitir organizar os dispositivos administrados em grupos: os sistemas virtuais deverão ser administrados como dispositivos individuais, os grupos podem ser geográficos, por funcionalidade (por exemplo, IPS), e distribuição;
9.12.15. Deverá permitir a criação de perfis de usuários com acesso a plataforma de gerenciamento com definição exata de quais informações e de qual firewall o usuário terá acesso referente a logs e relatórios;
9.12.16. Deverá permitir a criação de objetos e políticas compartilhadas;
9.12.17. Deverá permitir exportar backup de configuração automaticamente via agendamento;
9.12.18. Deverá permitir que a configuração do firewall seja importada de forma automática na plataforma de gerenciamento centralizado e que possa ser usada em outros firewalls e grupos de firewalls;
9.12.19. Deverá exibir o status do firewall em alta disponibilidade a partir da plataforma de gerenciamento centralizado;

9.13. Requisitos Técnicos

A contratada deverá prestar serviços de instalação e configuração da solução, que compreendem entre outros, os seguintes procedimentos:

9.13.1. Reunião de alinhamento para criação do escopo do projeto previamente a instalação;
9.13.2. Instalação física de todos os equipamentos (hardware) e licenças (software) adquiridas no local determinado pela equipe responsável pelo projeto por parte da contratante (Departamento de Tecnologia da Informação).
9.13.3. Análise da topologia e arquitetura da rede, considerando todos os equipamentos já existentes e instalados;
9.13.4. Análise do acesso à internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos;
9.13.5. Criação das regras de firewall aplicáveis à solução ofertada, considerando a adequação às políticas de aplicações em camada 7;
9.13.6. Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro pela solução;
9.13.7. Configuração do sistema de Firewall, VPN, IPS, Filtro URL, Antivírus e Anti-malware de acordo com as exigências levantadas;
9.13.8. Toda configuração de sistema (políticas gerais, objetos, itens de administração) deverá ser realizada de acordo com as melhores práticas recomendadas pelo fabricante da solução ofertada;
9.13.9. Durante a implantação da solução a equipe da Contratada deverá repassar as informações para a equipe de TI apresentando as configurações realizadas nos equipamentos, a topologia final e procedimentos executados;
9.13.10. O processo de implantação deverá ser devidamente documentado pela Contratada, que deverá apresentar relatório com o detalhamento do processo realizado ao final da implantação contendo todas as configurações efetuadas e as decisões tomadas em formato legível e tecnicamente fundamentado;
9.13.11. Os serviços de instalação e configuração deverão ser realizados por técnico certificado oficialmente pelo fabricante da solução ofertada ou pelo próprio fabricante;
9.13.12. A instalação física de todos os equipamentos (hardware) e licenças (software) adquiridos deverá ocorrer no local determinado pela equipe responsável pelo projeto por parte da contratante;

9.14. Treinamento de Firewall

9.14.1. A contratada deverá disponibilizar vouchers para treinamento oficial do fabricante ou equivalente;
9.14.2. O treinamento deverá ser ministrado abrangendo teoria e prática de implantação, configuração, administração e solução de problemas no ambiente deste órgão, bem como assuntos teóricos relacionados;
9.14.3. Deverá conter no mínimo a seguinte ementa:
9.14.3.1. Arquitetura da plataforma;
9.14.3.2. Configuração Inicial;
9.14.3.3. Configuração de Interface;
9.14.3.4. Políticas de Segurança e NAT;
9.14.3.5. Identificação de Aplicações;
9.14.3.6. Identificação de Conteúdo Básico;
9.14.3.7. Filtro de URL;
9.14.3.8. Decriptografia;
9.14.3.9. Sandboxing de ameaças avançadas;
9.14.3.10. Identificação de usuários;
9.14.3.11. VPN;
9.14.3.12. Monitoramento e Relatórios;
9.14.3.13. Configuração de Alta Disponibilidade (redundância);
9.14.3.14. Demais assuntos pertinentes a solução;
9.14.4. O treinamento deverá ser realizado pelo fabricante ou parceiro capacitado, de forma presencial ou vídeo conferência e deverá oferecer material didático e certificado de conclusão.

10. Qualificação Técnico-operaciona

10.1. Comprovação de aptidão para a prestação dos serviços similares de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso;
10.2. Para fins da comprovação de que trata o subitem anterior, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas, consideradas similares às do serviço que se pretende contratar:
10.2.1. Fornecimento de equipamentos NGFW;

10.2.2. Serviço de implantação das funcionalidades IPSEC VPN, SSL VPN, Firewall e Threat Prevention/Detection (com pelo menos IPS e antivírus/antimalware);

10.3. Será admitido, para fins de comprovação de quantitativo mínimo, o somatório de atestados;

10.4. Os atestados de capacidade técnica podem ser apresentados em nome da matriz ou da filial da empresa licitante;

10.5. Os atestados deverão conter, no mínimo:

10.5.1. Razão social, CNPJ e endereço da empresa ou órgão emitente;

10.5.2. Descrição detalhada dos serviços prestados;

10.5.3. Período de execução;

10.5.4. Avaliação do desempenho;

10.5.5. Assinatura do responsável técnico ou representante legal da emitente.

11. Parcelamento da Contratação

Fundamentação: Justificativas para o parcelamento ou não da solução. (Inciso VIII do § 1º do art. 18 da Lei 14.133/21 e art. 7º, inciso VII da IN 040/2020);

11.1. Para a solução em questão, a contratação em LOTE ÚNICO e a que melhor atende aos interesses dos órgãos da administração pública Municipal, pelas seguintes razões:

11.1.1. Por se tratar de locação de appliance e licença de software do mesmo fabricante como serviço, a fim de garantir a padronização e compatibilidade e gerir um único contrato;

11.1.2. O critério para seleção do fornecedor é aquele que atender 100% (cem por cento) das especificações técnicas e contratuais presentes no edital de licitação e ofertar o menor preço global;

11.1.3. O critério de julgamento pelo valor global foi adotado haja vista a complexidade da solução e a interdependência dos itens que a compõe. Ademais, a adjudicação deste objeto a um só fornecedor é uma forma de garantir a compatibilidade dos serviços prestados, trazendo eficiência e economicidade;

12. Resultados Pretendidos

Fundamentação: Demonstrativo dos resultados pretendidos em termos de economicidade e de melhor aproveitamento dos recursos humanos, materiais e financeiros disponíveis (inciso IX do § 1º do art. 18 da Lei 14.133/21). Resultados pretendidos, em termos de efetividade e de desenvolvimento nacional sustentável (Art. 7º, inciso X da IN 40/2020);

12.1. O resultado pretendido com a presente contratação visa muito mais do que apenas bloquear acessos indesejados. Ela representa uma estratégia robusta de segurança cibernética, com resultados bem definidos e alinhados às necessidades modernas da administração pública municipal. Dentre eles:

12.1.1. Segurança Avançada e Proativa

12.1.1.1. Proteção contra ameaças sofisticadas, como malware, ransomware, phishing e ataques de dia zero;

12.1.1.2. Inspeção profunda de pacotes (DPI) para identificar conteúdos maliciosos mesmo em tráfego legítimo;

12.1.1.3. Prevenção de Intrusões (IPS) integrada, com resposta automatizada a ataques;

12.1.2. Gestão Inteligente do Tráfego

12.1.2.1. Controle de aplicações para permitir ou bloquear softwares específicos com base em políticas;

12.1.2.2. Segmentação de rede para isolar áreas críticas e reduzir a superfície de ataque;

12.1.2.3. Qualidade de Serviço (QoS) para priorizar tráfego essencial e garantir desempenho;

12.1.3. Identificação e Controle de Usuários

12.1.3.1. Autenticação de usuários e visibilidade sobre quem acessa o quê;

12.1.3.2. Politicas baseadas em identidade, não apenas em IPs, para maior precisão;

12.1.4. Monitoramento e Respostas a Incidentes

12.1.4.1. Console de gerenciamento centralizado com logs detalhados e alertas em tempo real;

12.1.4.2. Capacidade de resposta rápida a incidentes, com relatórios e trilhas de auditoria;

12.1.5. Escalabilidade e Adaptabilidade

12.1.5.1. Suporte a ambientes complexos e em expansão, com alta capacidade de processamento;

12.1.5.2. Atualizações constantes para acompanhar o cenário de ameaças em evolução;

12.1.6. Continuidade dos Negócios

12.1.6.1. Minimização de riscos operacionais, garantindo que serviços essenciais não sejam interrompidos por ataques;

12.1.6.2. Preservação da reputação e conformidade com normas de segurança da informação;

13. Providencias a Serem Adotadas Previamente a Celebração do Contrato

13.1. Requisitos de Projeto e de Implantação

14. Requisitos de Projeto

14.1. Após a assinatura do contrato, a Contratada deverá marcar reunião inicial com a equipe técnica da Contratante para formulação do projeto para k*ickoff*, alinhamentos, levantamento de informações e quaisquer outras informações necessárias para elaboração de documentação inicial;

14.2. A Contratada deverá realizar uma avaliação preliminar do ambiente de TI da Contratante, incluindo uma análise da infraestrutura atual, para identificar quaisquer prerrequisitos ou necessidades de adaptação antes da implementação;

14.3. Deverá ser entregue Plano de Projeto, contendo, pelo menos, os seguintes artefatos: aspectos técnicos da implantação como detalhes de migração e procedimentos e teste a serem realizados;
14.4. A Contratada é responsável pela instalação completa e configuração dos equipamentos e softwares, garantindo que estes estejam operacionas e otimizados para o ambiente da Contratante;
14.5. A Contratada deverá manter um canal de comunicação aberto e contínuo com a Contratante, fornecendo relatórios regulares sobre o progresso da implementação, incluindo qualquer desafio ou desvio do plano original;
14.6. Toda reunião deverá gerar uma ATA que será assinada pela Contratada e Contratante;
14.7. As documentações geradas durante o projeto deverão ser entregues após o período de implantação;
14.8. Como exemplo, destacam-se as documentações técnicas referentes a configurações aplicadas, desenhos de arquitetura, identificação de interfaces/portas nos switches, políticas criadas e aplicadas (segurança, acesso, QoS, ETc.);
14.9. Junto as documentações técnicas, a Contratada deverá estabelecer um plano de recuperação de desastres com procedimentos claros para restaurar rapidamente os serviços em caso de falhas críticas ou eventos inesperados;

15. Requisitos de Implantação:

15.1. A implantação não deve interromper as operações diárias da CONTRATANTE e deve ser feita de forma a minimizar qualquer possível tempo de inatividade;
15.2. Todas as atividades realizadas deverão seguir as boas práticas sugeridas pelo fabricante da ferramenta, não sendo aceitas ações que não tenha respaldo documental;
15.3. A Contratada é responsável por quaisquer materiais para a implantação de serviço, por exemplo: Cabo par trançado, fibra óptica, transceivers, cabos de energia, adaptadores elétricos, velcro, cabo de crimpagem, etc.;
15.4. A Implantação envolverá as seguintes atividades:
15.4.1. Instalação física e lógica:
15.4.1.1. Deverá ser disponibilizado, em rack localizado no data center da Contratante, espaço físico para os novos equipamentos, utilizando-se dos PDUs existentes para cada PSU (Fonte de Energia). A fixação ocorrerá através de conjunto a ser fornecido junto com o equipamento;
15.4.1.2. Ao final a Contratada deverá providenciar relatório fotográfico da instalação física para envio à Contratante juntamente com a documentação gerada durante o projeto;
15.4.2. Configuração
15.4.2.1. Refere-se a configuração lógica do equipamento. Nesta etapa, as políticas, regras e quaisquer configurações do equipamento legado deverá ser migrada para o novo equipamento, além de criação de novas regras e políticas que se mostrem necessárias. Caso haja necessidade de rede para configuração, preferencialmente, o processo deverá ocorrer em ambiente apartado do ambiente produtivo, em rede virtual (VLAN) distinta do ambiente produtivo para que não haja influência na operação;
15.4.2.2. A Contratada deve validar os dados criados nos novos equipamentos comparando-os com os dados dos equipamentos legados, garantindo a integridade das configurações;
15.4.2.3. Os equipamentos devem ser configurados em 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;
15.4.2.4. Ao final, a Contratada deverá formalizar, por e-mail, a conclusão da configuração dos equipamentos da solução, indicando com prints de tela o que foi configurado, tão logo essa tarefa seja concluída;
15.4.3. Integração
15.4.3.1. Deverão ser conectados todos os cabos para o funcionamento pleno da ferramenta. Destaca-se que na etapa de configuração, somente os cabos necessários para configuração serão conectados;
15.4.3.2. A Contratada ficará responsável pela organização e identificação (etiquetagem) de todos os cabos (rede, óptico e/ou elétricos) que serão utilizados e instalados na infraestrutura da Contratante;
15.4.3.3. A integração deve ser efetuada de maneira a não interromper as operações existentes e serviços. A abordagem de como será feita deverá ser descrita no plano de projeto;
15.4.4. Testes
15.4.4.1. Os testes têm por objetivo validar que todos os requisitos solicitados e apresentados na proposta da Contratada estão sendo atendidos;
15.4.4.2. Os testes serão, preferencialmente, realizados em ambiente lógico apartado da rede produtiva da Contratante;
15.4.4.3. Deverão ser realizados, pelo menos, os seguintes tipos de teste: penetração (pen test), desempenho, segurança funcional, resiliência e escalabilidade;
15.4.4.4. Como testes de penetração entende-se a simulação de ataques reais conto o NGFW para identificar e explorar vulnerabilidades. Como por exemplos, testes de by-pass de Firewall (Tráfego camuflado, túneis e/ou encapsulamento), exploração de vulnerabilidades conhecidas, injeção de pacotes maliciosas, analise de tráfego criptografado (esconder atividades maliciosas dentro de tráfego criptografado) etc.
15.4.4.5. Como teste de desempenho entende-se avaliar a capacidade do NGFW e um servidor virtual localizado na rede interna, verificar o máximo de carga que os equipamentos suportam em relação a throughput e conexões simultâneas solicitadas, verificar a latência de resposta RTT (Round-Trip Time) entre o NGFW e um servidor virtual localizado na rede interna, verificar o máximo de carga que os equipamentos suportam em relação a throughput e conexões simultâneas (sobrecarga de conexões) dentro das limitações da rede interna, inspeção profunda de pacotes (deep package inspection) com a capacidade do NGFW analisar análises detalhadas de pacotes (relacionado aos testes de penetração), validar quantidade de conexões na VPN IPSEC e SSL etc;
15.4.4.6. Como teste de configuração funcional entende-se verificar as funcionalidades solicitadas pela Contratante como firewall, IPS/IDS, controle de aplicações QoS, antivírus ou malware descriptografia e inspeção de tráfego SSL/TLS, filtro de

conteúdo, VPN IPSEC/SSL. Como exemplos, verificar intrusões (validado durante o pen test), validar se sites proibidos (adultos, apostas, pirataria etc.) são bloqueados, validar bloqueio de tráfego através de inspeção SSL/TLS (validado durante o pen test), verificar prevenção de ameaças avançadas através de evasão de assinatura em que um malware conhecido sofra metamorfose e o NGFW é capaz de identificar esse comportamento e bloquear, validar as políticas criadas e migradas alterando a ordem e percebendo o comportamento da ferramenta, validar se as regras de QoS estão sendo aplicadas corretamente comparando o comportamento da ferramenta quando estas são desativadas etc;

15.4.5. Teste de funcionalidades entre redes

15.4.5.1. O objetivo é verificar se o Firewall consegue liberar determinados protocolos a uma rede específica.

15.4.5.2. Deve ser feito dois tipos de acesso a partir da rede interna para rede servidores e para rede DMZ;

15.4.5.3. Acesso 1: utilizando protocolo https e sendo liberado o acesso;

15.4.5.4. Acesso 2: utilizando ssh e sendo bloqueado para a DMZ e liberado para a rede servidores;

15.4.5.5. Deverá ser feito um tipo de acesso externo com origem em um cliente VPN (que deverá ser configurado) com destino a rede servidores;

15.4.6. Teste de funcionalidades de auditoria

15.4.6.1. O objetivo é mostrar que a solução é capaz de mostrar as informações detalhadas de auditoria sobre mudanças realizadas;

15.4.6.2. Deverá ser exibido na console de gerência os registros que demonstrem, o horário da aplicação das últimas políticas, a mudança realizada para bloqueio do facebook, o horário da mudança e o administrador que realizou a mudança;

15.4.7. Teste de funcionalidades de desempenho do IPS;

15.4.7.1. O objetivo é verificar o comportamento na ferramenta com a funcionalidade IPS ativa e se atinge os requisitos mínimos de throughput solicitados;

15.4.7.2. A Contratada deverá utilizar alguma solução de geração de tráfego com o intuito de gerar diversos tipos de ataque contra a solução a fim de validar que as assinaturas estão habilitadas e realizando devidamente os bloqueios;

15.4.7.3. Os ataques a serem simulados serão feitos como se estivessem conectados vindos da internet;

15.4.7.4. A partir da gerência do appliance deva ser possível verificar os logs das tentativas de acesso malsucedidas;

15.4.7.5. A Contratada deverá também demonstrar quais assinaturas foram utilizadas durante a sessão de teste;

15.4.7.6. A Contratada deverá realizar testes de simulação com ataques diversos com o intuito de validar, minimamente, que o IPS/IDS funciona a contento com diversas assinaturas ativadas e diversos ataques realizados simultaneamente;

15.4.8. Documento modelo a ser adotado para os testes

CENÁRIO DE TESTE	CONDIÇÃO DE ENTRADA	CONDIÇÃO DE SAÍDA	RESULTADO ESPERADO	STATUS

15.4.9. Operação assistida

15.4.9.1. É o período em que uma mão de obra da Contratada ficará alocada nas dependências da Contratante, monitorando as atividades dos equipamentos hora locados pelo período de 30 dias corridos. Caso seja necessário, deverão ser aplicadas configurações de tunning para melhoria de desempenho e/ou disponibilidade.

15.4.9.2. Os acionamentos da Contratada pela Contratante, durante o período de operação assistida, deverão ser tratados com o nível de serviço definidos para prioridade alta da tabela de Nível Mínimo de Serviços;

15.4.9.3. A operação assistida iniciará após a finalização do processo de testes;

15.4.9.4. A critério da Contratante, a operação assistida poderá ser na modalidade presencial, híbrida ou remota;

15.4.10. Encerramento:

15.4.10.1. A Contratada deverá comprovar o registro no portal da fabricante dos partnumbers, ou similar, que compõem a solução, se aplicável;

15.4.10.2. É o período em que o projeto se encerra com a emissão do Termo de Recebimento Definitivo de Implantação.

16. Requisitos de Garantia

16.1. **Garantia Contratual dos Serviços:** O prazo de garantia contratual dos serviços (suporte técnico), complementar à garantia legal, será de no mínimo 60 (sessenta) meses, contado a partir da assinatura do Termo de Recebimento Definitivo da Ativação de Licenças. Esta garantia é exigida para assegurar a prestação continuada de serviços com a qualidade esperada e a correção de possíveis defeitos ou falhas que possam surgir durante o período estabelecido. Ressalta-se que durante a fase de implantação (instalação, configuração, integração, testes e operação assistida), caso haja necessidade de licenças válidas, deverão ser fornecidas licenças provisórias por parte da Contratada para a Contratante, não sendo considerados os 60 meses. Essas licenças provisórias deverão ter as mesmas características das licenças definitivas hora locadas pela Contratante. Caso não haja possibilidade, as licenças deverão ter seu período estendido durante a fase de implantação para que não seja afetado o período de 60 meses;

16.2. **Garantia Contratual dos Bens:** Considerando que os serviços envolvem o fornecimento de equipamentos de alta criticidade para a segurança da informação e infraestrutura de rede da Contratante, a garantia contratual dos bens (hardware) será de no mínimo, 60 (sessenta) meses, contados a partir da emissão do Termo de Recebimento Definitivo da Ativação de Licenças. Este período visa cobrir quaisquer defeitos de fabricação, funcionamento inadequado ou outras falhas que possam comprometer a integridade do sistema e a continuidade dos serviços públicos prestados pela instituição. Ressalta-se que durante a fase de implantação (instalação, configuração, integração, testes e operação assistida), os equipamentos deverão possuir garantia legal e/ou provisória, não sendo considerados dentro dos 60 meses;

16.2.1. A Contratada deverá prover para a Contratante um usuário para utilização de portal de suporte técnico

16.2.2. Serão aceitos modelo de suporte hibrido, em que os primeiros níveis são atendidos pela Contratada e os últimos níveis pelo Fabricante do equipamento;

16.2.3. Encargos de Garantia: Toso os custos e encargos relacionados à execução dos serviços de garantia contatual e assistência técnica necessários durante o prazo de garantia dos serviços e dos bens serão de responsabilidade integral da Contratada, sem oneração adicional para a Contratante;

17. Requisitos de Experiência Profissional

17.1. Os serviços de assistência técnica e garantia deverão ser prestados por técnicos da Contratada ou da Fabricante;

17.2. A Licitante provisoriamente vencedora do certame deverá apresentar declaração formal de que irá disponibilizar profissional responsável pelo serviço de operação e sustentação, respeitando as especificações em que esse serviço está definido;

17.3. A Licitante deverá apresentar comprovação da capacitação dos profissionais através de apresentação de documentação ou certificados emitidos pela fabricante da solução. A comprovação poderá ser feita por meio de certificados de participação em treinamento ou carta emitida pela fabricante do produto;

17.4. O profissional responsável por prover o serviço agregado de operação e sustentação do ambiente deverá ter certificação do fabricante em relação aos produtos fornecidos pela Contratada ou ser funcionário vinculado ao fabricante do produto. Caso não haja certificação para as ferramentas, serão aceitos certificados de conclusão de treinamento com atestado(s) que comprovem as atividades de operação relacionadas às ferramentas adquiridas;

17.5. A exigência de capacidade técnica acima e experiência prévia tem por objetivo comprovar experiência anterior na realização de serviços similares, proporcionais à dimensão e complexidade do objeto a ser executado, visando assegurar que a Administração contratará empresas e profissionais que possam incumbir-se adequadamente do objeto contratado. Os equipamentos envolvidos na especificação desta contratação tratam de tecnologias (protocolos) complexos, como VPN IPSEC, SSL VPN, Threat Detection, análise de vulnerabilidades em arquivos e dados. Estes equipamentos, se mal configurados, podem indisponibilizar a comunicação segura entre a Prefeitura Municipal de Paraguaçu Paulista e o mundo externo, incluindo, mas não se limitando, a tráfego com usuários em teletrabalho, outras entidades públicas e privadas, usuários externos que acessam informações em sistemas de atendimento à população e usuários internos que necessitam acessar serviços externos. Também destacamos que a má configuração dos equipamentos pode, ainda, expor a rede de dados do Município a ataques externos que visam extrair dados ou gerar indisponibilidade dos serviços desta instituição. Os conhecimentos técnicos necessários para implementar as tecnologias acima não são triviais e exigem conhecimento prévio e comprovado das tecnologias do produto;

18. Requisitos de Níveis de Serviço

18.1. Os níveis mínimos de serviço esperados para esta contratação, bem como para os atendimentos aos incidentes/eventos associados estão indicados na Tabela – Níveis Mínimos de Serviço;

18.2. Todos os prazos para a resolução dos incidentes/eventos especificados na Tabela – Níveis Mínimos de Serviço são contados a partir da abertura (registro) do chamado;

18.3. A abertura do chamado com fornecimento do seu número de identificação (protocolo de atendimento) a partir da tentativa de contato pela Contratante com o número fornecido pela Contratada deve ocorrer no prazo máximo de:

18.3.1. 30 (trinta) minutos, se severidade Alta ou Média;

18.3.2. 60 (sessenta) minutos, se severidade Baixa;

18.4. O prazo de Resolução do problema dar-se-á a partir do registro do chamado, seja de forma automática, pela ferramenta da Contratada, ou pela Contratante;

18.5. Para atendimentos presenciais, o tempo de deslocamento do funcionário da Contratada será considerado dentro do prazo de resolução do incidente;

18.6. A severidade deve levar em conta o fator que foi usado na sua abertura e seguir esse mesmo critério até a sua completa solução. O chamado poderá ser reclassificado pela Contratante de acordo com a criticidade do problema;

18.7. A expressão “dia-útil” refere-se ao período das 7:30h as 17:00h, de segunda a sexta-feira, excluindo-se feriados que venham a coincidir com este período;

18.8. Tabela de Níveis Mínimos de Serviço:

Severidade	Classificação	Tempo de Atendimento	Prazo de Resolução
(A). Alta	São consideradas como “ALTA” todas as falhas cujas consequências tenham impactos negativos e severos, gerando indisponibilidade sobre o serviço e o tráfego e/ou recursos. São situações que exijam atenção imediata. Exemplo: Situação de indisponibilidade total do equipamento, funcionamento intermitente ou parcial do equipamento, que possa levar à interrupção intermitente ou total de serviços ou perda de tráfego	O prazo para início do atendimento após registro formal da ocorrência será de 30 minutos	4,5 horas corridas com solução definitiva ou aplicação de medida de contorno que permita estabilização do ambiente para posterior solução definitiva
(B). Média	Problemas que não prejudicam significativamente o funcionamento dos sistemas/serviços dos equipamentos. São problemas sérios ou perturbações, que afetam uma	O prazo para início do atendimento após o registro formal da ocorrência será de 30 minutos	O prazo para atendimento com solução definitiva será de 8,5 horas corridas

	área especifica ou determinada funcionalidade do equipamento. Configurações emergenciais para atender requisitos do negócio serão classificadas como média. Exemplo: Reinicialização de módulos, slots ou portas com defeitos, degradação de desempenho, perda de funcionalidades, bloqueios de tráfego indevidos, criação ou ajustes de políticas para atender demandas inesperadas		
(C). Baixa	Solicitação de informações sobre o funcionamento dos equipamentos, possíveis configurações ou usos, que não gerem interrupções, nem indisponibilidade de determinada área ou uma funcionalidade específica.	O prazo para início do atendimento após registro formal da ocorrência será de 60 minutos	O prazo para atendimento com solução definitiva ou de contorno será de 48 horas corridas

18.9. Serão aceitos par atendimento e cumprimento dos prazos acima indicados o suporte direto do fabricante, sem o direito de isenção de responsabilidade pela Contratada.

19. Requisitos de Sustentabilidade

19.1. O licitante provisoriamente classificado em primeiro lugar deverá apresentar juntamente com a proposta comprovação de que os bens ofertados não contêm substâncias perigosas em concentração acima das recomendadas na diretiva RoHS.

19.2. Vale destacar que é impossível identificar no ETP todos os materiais recicláveis possíveis de serem utilizados nas embalagens dos equipamentos, pois há muitos tipos e formas de materiais recicláveis. É comum que os equipamentos venham embalados em caixas de papelão ou papel, mas no interior estejam acondicionados em embalagens de isopor e plástico, sendo os referidos materiais também recicláveis e podem ser admitidos como critérios de sustentabilidade. Desse modo, prever apenas um tipo de material sem atentar para as diversidades de mercado poderá comprometer a competitividade do certame.

20. Contratações Correlatas e/ou Interdependentes

20.1. Não foram detectadas necessidades de contratações correlatas e/ou interdependentes;

21. Conclusão da Viabilidade da Contratação

21.1. **Fundamentação:** Posicionamento conclusivo sobre a adequação da contratação para o atendimento da necessidade a que se destina (inciso XIII do § 1º do art. 18 da Lei 14.133/21). Posicionamento conclusivo sobre a viabilidade e razoabilidade da contratação (Art. 7º, inciso XIII da IN 40/2020).

21.1.1. Conforme fundamentação acima, considerar, que a solução de Tecnologia da Informação e Comunicação escolhida é viável com base nos elementos anteriormente apresentados neste Estudo Técnico Preliminar, além de ser necessária para o atendimento das necessidades e interesses dos órgãos da administração Pública Municipal;

Servidores Responsáveis Pela Elaboração	Secretária
Wilson Spavier Diretor do Departamento de Tecnologia da Informação	Tatiani dos Santos Correa Secretária Municipal de Planejamento

Paraguaçu Paulista, na data da assinatura digital.

[NOME DO SIGNATÁRIO]
[Cargo do signatário]

Documento assinado eletronicamente por **Wilson Spavier**, **Diretor do Departamento de Tecnologia da Informação**, em 31/10/2025, às 07:44, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023 e Decreto Municipal de regulamentação do processo eletrônico.

Documento assinado eletronicamente por **Tatiani dos Santos Correa**, **Secretário Municipal**, em 31/10/2025, às 08:04, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023 e Decreto Municipal de regulamentação do processo eletrônico.

A autenticidade deste documento pode ser conferida no site https://cidades.sei.sp.gov.br/marilia/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0113546** e o código CRC **BD0C1D0A**.