TERMO DE REFERÊNCIA

PROCESSO ADMINISTRATIVO 091/2025

SIGILO: ( ) SIM (X) NÃO PREVISÃO NO PCA: (X) SIM ( ) NÃO

1 - ÁREA DEMANDANTE

Departamento Demandante: Secretaria de Administração	
Chefe Setor: Marcieli Gomes	
E-mail (Institucional): administrativo@sinop.mt.leg.br	**Telefone (Institucional):** 66.3517-2810

2 – OBJETO

2.1 ESPECIFICAÇÕES DO OBJETO:

"CONTRATAÇÃO DE EMPRESA ESPECIALIZADA EM SERVIÇOS DE BACKUP LEGISLATIVO, CONFIGURAÇÃO DE FIREWALL E CIBERSEGURANÇA COM CAPTIVE PORTAL", PARA ATENDER AS NECESSIDADES DO SETOR CPD DA CÂMARA MUNICIPAL DE SINOP.

2.2 DESCRIÇÃO E QUANTIDADES

( ) os itens, as descrições e suas quantidades seguem em anexo.

(X) os itens, as descrições e suas quantidades seguem abaixo.

ITEM	COD	DESCRIÇÃO E ESPECIFICAÇÃO	UN. MED	QTD	VLR UNIT. ESTIMADO	VLR TOTAL ESTIMADO
1	19429	PRESTAÇÃO DE SERVIÇOS GERENCIADOS DE CIBERSEGURANÇA COM CAPTIVE PORTAL E FIREWALL CONTEMPLANDO SUBSCRIÇÃO E SUPORTE TÉCNICO REMOTO	MÊS	12	R$ 4.803,75	R$ 57.645,00
2	19428	SERVIÇOS ESPECIALIZADOS DE SEGURANÇA DA INFORMAÇÃO COM BACKUP EM NUVEM;	MÊS	12	R$ 2.193,33	R$ 26.319,96

Valor Total: R$ 83.964,96 (Oitenta e três mil e novecentos e sessenta e quatro reais e noventa e seis centavos**).**

3 – JUSTIFICATIVA/NECESSIDADE DA CONTRATAÇÃO

3.1 Importa destacar que esta contratação foi inicialmente objeto de processo **Pregão Eletrônico Nº 009/2025**, o qual foi cancelado por iniciativa do Pregoeiro, em razão do acolhimento de pedido de impugnação, devidamente analisado e deferido, o que motivou o cancelamento do certame para adequações necessárias nos termos do questionamento apresentado.

3.2. Assim, a Câmara Municipal de Sinop promoveu a devida revisão do instrumento convocatório, realizando os ajustes pertinentes com base nas observações apontadas, assegurando o princípio da legalidade, da competitividade e da ampla participação. A reabertura do processo licitatório com as devidas correções visa garantir maior segurança jurídica ao procedimento, bem como a contratação de serviços que são imprescindíveis para o

funcionamento seguro e eficiente da infraestrutura de tecnologia da informação da Casa Legislativa.

3.3. A crescente digitalização das operações na administração pública, aliada ao aumento das ameaças cibernéticas, exige que a Câmara Municipal adote medidas robustas para proteger suas informações sensíveis, dados de cidadãos e processos administrativos. O gerenciamento de cibersegurança eficaz é essencial para garantir a continuidade das atividades da instituição, proteger a integridade da infraestrutura de TI e assegurar a conformidade com as legislações pertinentes. Nesse contexto, a aquisição de serviços gerenciados de cibersegurança que incluem firewall, captive portal, subscrição e suporte técnico remoto se torna uma medida estratégica e necessária para atender às exigências legais, garantir a proteção da rede e melhorar a gestão da segurança da informação.

3.4. A Câmara Municipal como qualquer instituição pública é alvo constante de ameaças cibernéticas como ransomware, phishing, ataques DDoS e invasões maliciosas. Esses ataques não apenas comprometem a segurança dos dados, mas também podem paralisar as operações essenciais do Órgão afetando a confiança da população e a continuidade dos serviços públicos. A implementação de um firewall gerenciado proporciona uma camada de proteção fundamental, controlando o tráfego de rede, bloqueando acessos não autorizados e prevenindo tentativas de invasão. Além disso, o firewall realiza inspeções profundas dos pacotes de dados, detectando e bloqueando ameaças antes que causem danos à infraestrutura da Câmara.

3.5. O captive portal complementa a proteção permitindo que apenas usuários autenticados tenham acesso à rede sem fio da Câmara, garantindo que as conexões externas como de visitantes ou fornecedores, sejam monitoradas e autorizadas, evitando qualquer acesso não autorizado ou riscos associados ao uso indevido da rede.

3.6. A segurança da informação na administração pública deve atender a várias normas e regulamentações legais que garantam a privacidade e proteção dos dados pessoais. A Lei Geral de Proteção de Dados Pessoais (LGPD) e o Marco Civil da Internet são algumas das legislações que exigem que as entidades públicas adotem práticas rigorosas para proteger os dados dos cidadãos e garantir a confidencialidade das informações processadas.

3.1.7 A LGPD (Lei nº 13.709/2018) estabelece diretrizes claras para o tratamento e proteção dos dados pessoais tanto em organizações privadas quanto públicas. No contexto da Câmara Municipal que lida com dados de cidadãos, servidores públicos e processos administrativos, a LGPD exige que sejam adotadas medidas de segurança eficazes para proteger essas informações contra acessos não autorizados, vazamentos e incidentes de segurança.

3.1.8 De acordo, com o artigo 46 da LGPD é responsabilidade do controlador (Câmara Municipal) Implementar medidas técnicas e administrativas para proteger os dados pessoais. A aquisição de firewall gerenciado e a Implementação de captive portal garantem a proteção da rede que é uma exigência da lei para a prevenção de incidentes de segurança que possam comprometer dados pessoais. O suporte contínuo e as atualizações fornecidas pelo serviço de subscrição garantem que a infraestrutura de segurança esteja sempre em conformidade com as melhores práticas e atualizada de acordo com as novas ameaças.

3.1.9 O Marco Civil da Internet (Lei nº 12.965/2014) em seu artigo 10, impõe a responsabilidade de provedores de serviços de internet em relação à segurança e privacidade dos dados dos usuários. Ao adotar um sistema gerenciado de cibersegurança a Câmara estará

em conformidade com essa exigência, garantindo que os dados e as comunicações dos cidadãos que acessam a rede institucional sejam devidamente protegidos. O firewall e o captive portal proporcionam não apenas a proteção dos dados, mas também a privacidade dos usuários ao garantir que o acesso à rede seja controlado e monitorado.

3.1.10 A Lei de Acesso à Informação (LAI) (Lei nº 12.527/2011) estabelece que órgãos públicos devem garantir o acesso à informação de maneira transparente, mas também precisa assegurar a proteção de dados sensíveis. A utilização de um firewall gerenciado e captive portal impedem o acesso indevido a informações confidenciais ou de caráter sensível, alinhando-se às obrigações de garantir o acesso seguro aos dados, conforme estabelecido pela LAI.

3.1.11 A gestão contínua de segurança cibernética exige monitoramento em tempo integral, detecção de ameaças em tempo real e capacidade de resposta rápida a incidentes. A subscrição de um serviço gerenciado de cibersegurança garante que a Câmara Municipal tenha acesso a uma infraestrutura de segurança de ponta sem a necessidade de manter uma equipe interna dedicada exclusivamente a essas funções. O suporte técnico remoto especializado oferece atendimento imediato em caso de incidentes ou falhas de segurança, reduzindo os riscos de danos e permitindo uma resposta mais eficiente.

3.1.12 O serviço de suporte remoto oferece a vantagem de não precisar de deslocamento físico, economizando tempo e recursos. Além disso, os especialistas responsáveis pelo gerenciamento da cibersegurança monitoram a rede em tempo integral, realizando análises detalhadas e implementando ajustes de segurança conforme necessário. A constante atualização das políticas de segurança realizada por meio da subscrição assegura que o sistema esteja sempre preparado para enfrentar novas ameaças.

3.1.13 A subscrição do serviço de cibersegurança gerenciado com suporte remoto e firewall permite à Câmara Municipal reduzir significativamente os custos operacionais em comparação com a contratação de uma equipe interna especializada e a aquisição de equipamentos próprios. A Implementação de uma solução escalável e de baixo custo inicial permite que a Câmara proteja sua infraestrutura de TI de maneira eficaz sem a necessidade de investimentos pesados em hardware ou infraestrutura adicional. Além disso, o serviço gerenciado oferece flexibilidade para aumentar ou ajustar os recursos de segurança conforme a evolução das necessidades da Câmara o que proporciona uma escala de proteção ajustável à medida que a instituição cresce ou enfrenta novos desafios de segurança.

3.1.14 A segurança da informação não se refere apenas à proteção de dados, mas também à proteção da imagem institucional. Caso a Câmara sofra um ataque cibernético, os danos à reputação podem ser irreparáveis, afetando diretamente a confiança da população. Ao adotar medidas proativas de segurança como a aquisição de um firewall gerenciado e captive portal a Câmara Municipal demonstra seu compromisso com a proteção dos dados dos cidadãos e com a segurança das informações. Isso fortalece a confiança do público nas operações da instituição e assegura a continuidade dos serviços essenciais para a população.

3.1.15 Além do mais restam imperiosos que os gestores públicos promovam a capacitação da equipe, através de campanhas de utilização dos meios digitais, haja vista que, a exploração das vulnerabilidades humanas, através de engenharia social, perfaz o caminho mais utilizado pelos criminosos cibernéticos, razão pela qual, necessária a contratação de plataforma que promova a educação digital dos servidores da Câmara Municipal de Sinop-MT.

3.2 – BACKUPS LEGISLATIVOS

3.2.1 O backup dos dados legislativo para a Câmara Municipal é uma medida essencial para garantir a segurança, integridade e recuperação de dados sensíveis, conforme exigências legais e normativas. A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 - LGPD) impõe a obrigatoriedade de proteção e governança das informações, determinando que órgãos públicos adotem medidas de segurança para evitar acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração e difusão de dados.

3.2.2 Além disso, a Lei de Acesso à Informação (Lei nº 12.527/2011) estabelece a necessidade de garantir a transparência e preservação de documentos públicos, exigindo que os dados sejam protegidos contra qualquer risco de indisponibilidade.

3.2.3 Nos termos do artigo 11 da referida lei, a contratação pública deve observar entre outros, os princípios da eficiência, da transparência e do interesse público, sendo vedada a celebração de contratos que não estejam amparados por justificativa de necessidade concreta, o que é plenamente evidenciado neste caso. A implantação de uma política de backup adequada por meio de empresa especializada atende também ao artigo 6º, inciso XXV, que define como serviços técnicos especializados aqueles que demandam conhecimentos específicos, como é o caso da gestão de dados digitais e políticas de segurança da informação.

3.2.4 A escolha da empresa prestadora do serviço deverá considerar critérios como experiência e certificações na área de backup e segurança da informação, capacidade técnica para atender às necessidades da Câmara Municipal, nível de segurança e conformidade com as normas legais, qualidade do suporte técnico oferecido e tempo de resposta para a recuperação de dados, além do custo-benefício e condições contratuais adequadas à administração pública. A contratação seguirá os trâmites legais estabelecidos pela legislação vigente, incluindo a elaboração do Termo de Referência com a definição dos requisitos técnicos e operacionais do serviço, abertura de processo licitatório conforme as normas da Lei nº 14.133/2021 ou, quando aplicável, dispensa de licitação justificada, seleção da empresa com melhor proposta técnica e financeira, formalização do contrato e início da prestação dos serviços, além do monitoramento contínuo da execução do serviço, com auditorias e testes periódicos para garantir a eficácia do backup.

3.2.5 Diante dessas normativas, a contratação de um serviço especializado de backup é imprescindível para garantir a continuidade dos serviços da Câmara Municipal, protegendo dados estratégicos contra: ataques cibernéticos, falhas técnicas e desastres, assegurando a disponibilidade e integridade das informações legislativas.

4 – DESCRIÇÃO DA SOLUÇÃO (QUANDO APLICÁVEL)

Natureza do Objeto: Conforme definido pelo Art. 6°, inciso XIII, da Lei 14.133/21, trata-se de bens e serviços comuns, cujos padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado.

4.1. A contratação de serviços especializados em Backups legislativos, configuração de Firewall gerenciados de cibersegurança com a inclusão de captive portal**,** subscrição e suporte

técnico remoto para a Câmara Municipal deve atender a uma série de requisitos técnicos, legais e operacionais, com o objetivo de garantir a segurança da rede institucional, a proteção dos dados dos cidadãos e a conformidade com as legislações pertinentes.

4.2. A solução consiste na realização de processo licitatório, com o objetivo de atender a Câmara Municipal de Sinop-MT e seus departamentos, permitindo assim a decisão da contratação dos serviços com base no menor preço.

4.3. Os serviços deverão ser realizados na Câmara Municipal de Sinop, em horário de expediente (07h às 13h), sendo recebidos pelo agente do setor de Administração de Rede e posteriormente conferidos pelo fiscal do contrato.

4.4. Prestar todos os esclarecimentos que forem solicitados pela Contratante, obrigando-se a atender todas as reclamações a respeito da qualidade e eventuais substituições.

4.5. A contratação de serviços especializados em Backups legislativos e configuração de Firewall gerenciados de cibersegurança com a inclusão de captive portal**,** subscrição e suporte técnico remoto para a Câmara Municipal deve atender a uma série de requisitos técnicos, legais e operacionais, com o objetivo de garantir a segurança da rede institucional, a proteção dos dados dos cidadãos e a conformidade com as legislações pertinentes.

5 – REQUISITOS DO OBJETO DA CONTRATAÇÃO

5.1 A CONTRATADA deverá prestar serviços especializados de segurança da informação, constante no Termo de Referência, dentro do padrão técnico e melhores práticas de mercado, considerando as seguintes aplicações e soluções:

a) Solução NGFW/SD-Wan em appliance compatível com especificações;

b) Mapeamento de vulnerabilidades;

c) Captive portal;

d) Solução de gerenciamento de Logs;

e) Controlador de usuários (Microsoft Active Directory – AD Licenciado);

f) Fornecimento de plataforma de campanhas de Phishing e treinamento em proteção de dados;

g) Fornecimento de solução de backup.

5.2 Características Técnicas dos equipamentos e dos serviços especializados de segurança da informação:

5.2.1 Deve possuir interface de console serial via RJ45 ou USB;

5.2.2 Deve possuir no mínimo 1 (uma) interface RJ45-UTP dedicada ao gerenciamento out of

band;

5.2.3 Deve possuir no mínimo 8 (oito) interfaces RJ45-UTP, podem ser fornecidas interfaces SFP desde que com transceiver RJ45;

5.2.4 Throughput de Firewall de no mínimo 28 (vinte e oito) Gbps;

5.2.5 Throughput de Prevenção de Ameaças (funcionalidades ativas de: Firewall, Controle de Aplicação, IPS, Proteção contra Malware) de no mínimo 2.2 (dois ponto dois) Gbps;

5.2.6 Throughput de VPN IPSec de no mínimo 25 (vinte e cinco) Gbps;

5.2.7 Permitir o número de túneis VPN IPSEC Site-to-Site mínimo de 200 (duzetos);

5.2.8 Permitir o número de túneis VPN IPSEC Client-to-Site mínimo de 2500 (dois mil e quinhentos);

5.2.9 Permitir o número de túneis/usuários VPN SSL mínimo de 200 (duzentos);

5.2.10 Throughput de inspeção SSL de no mínimo 2.6 (dois ponto seis) Gbps;

5.2.11 Permitir no mínimo 1.5 (um ponto cinco) mil sessões TCP Concorrentes;

5.2.12 Permitir no mínimo 124 (cento e vinte e quatro) mil novas conexões TCP por segundo;

5.2.13Permitir no mínimo 10 (dez) Firewalls virtuais;

5.2.14 Deve suportar e implementar tags de VLAN;

5.2.15 Deve permitir a criação de no mínimo 200 VLANs padrão 802.1q nos equipamentos NGFW;

5.2.16 Deve possuir funcionalidades de: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

5.2.17 As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;

5.2.18 A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

5.2.19 A gestão do equipamento deve ser compatível através da interface de gestão Web no mesmo dispositivo de proteção da rede;

5.2.20 Os dispositivos de proteção de rede devem possuir suporte a Policybasedrouting ou policybasedforwarding;

5.2.21 Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

5.2.22 Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;

5.2.23 Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;

5.2.24 Os dispositivos de proteção de rede devem suportar sFlow;

5.2.25 Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;

5.2.26 Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;

5.2.27 Deve suportar NAT dinâmico (Many-to-1);

5.2.28 Deve suportar NAT dinâmico (Many-to-Many);

5.2.29 Deve suportar NAT estático (1-to-1);

5.2.30 Deve suportar NAT estático (Many-to-Many);

5.2.31 Deve suportar NAT estático bidirecional 1-to-1;

5.2.32 Deve suportar Tradução de porta (PAT);

5.2.33 Deve suportar NAT de Origem;

5.2.34 Deve suportar NAT de Destino;

5.2.35 Deve suportar NAT de Origem e NAT de Destino simultaneamente;

5.2.36 Deve poder combinar NAT de origem e NAT de destino na mesma política;

5.2.37 Deve implementar Network PrefixTranslation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

5.2.38 Deve suportar NAT64 e NAT46;

5.2.39 Deve implementar o protocolo ECMP;

5.2.40 Deve suportar SD-WAN de forma nativa;

5.2.41 Deve implementar balanceamento de link por hash do IP de origem;

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

5.2.43 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;

5.2.44 Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;

5.2.45 Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;

5.2.46 Enviar log para sistemas de monitoração externos, simultaneamente;

5.2.47 Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;

5.2.48 Proteção anti-spoofing;

5.2.49 Implementar otimização do tráfego entre dois equipamentos;

5.2.50 Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

5.2.51 Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

5.2.52 Suportar OSPF gracefulrestart;

5.2.53 Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

5.2.54 Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;

5.2.55 Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;

5.2.56 Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

5.2.57 Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;

5.2.58 Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3;

5.2.59 Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster;

5.2.60 A configuração em alta disponibilidade deve sincronizar: Sessões;

5.2.61 A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QoS e objetos de rede;

5.2.62 A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;

5.2.63 A configuração em alta disponibilidade deve sincronizar:Tabelas FIB;

5.2.64 O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;

5.2.65 Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;

5.2.66 Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;

5.2.67 O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado a exportar configuração dos sistemas virtuais (contextos) por ambas interfaces;

5.2.68 Controle, inspeção e descriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);

5.2.69 Deve ser fornecido funcionalidade de Inspeção SSL sem limitação de licenciamento

caso a solução ofertada possua licenciamento, deve ser fornecido em sua capacidade máxima.

5.2.70 Permitir a integração com repositório de logs de forma segura e otimizada;

5.2.71 Permitir identificar potenciais vulnerabilidades ou ameaças e orquestrar ação de prevenção.

5.2.72 Deve existir um Serviço de Suporte que ofereça apoio do fabricante e atualização de sistema operacional;

5.2.73 A console de administração deve suportar no mínimo inglês, espanhol e português.

5.2.74 A console deve suportar a administração de switches e pontos de acesso para melhorar o nível de segurança;

5.2.75 A solução deve suportar integração nativa de equipamentos de proteção de correio eletrônico, firewall de aplicações, proxy, cache e ameaças avançadas

5.2.76 Deverá suportar controles por zona de segurança;

5.2.77 Controles de políticas por porta e protocolo;

5.2.78 Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;

5.2.79 Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

5.2.80 Deve ser capaz de aplicar a inspeção ApplicationControl e Webfiltering no mínimo e diretamente às políticas de segurança versus via perfis;

5.2.81 Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados diretamente as políticas de firewall;

5.2.82 Deve suportar automação de situações como detecção de equipamentos comprometidos, estado do sistema, mudanças de configuração, eventos específicos, e aplicar uma ação que possa ser notificação, bloqueio do equipamento, execução de scripts ou funções em nuvem pública.

5.2.83 Deve suportar o padrão de indústria 'syslog' protocol para armanazemento usando o formato Common Event Format (CEF);

5.2.84 Deve suportar integração de nuvens públicas e integração SDN como AWS, Azure, GCP, OCI, AliCloud, VmwareESXi, NSX, OpenStack, Cisco ACI, Nuage e Kubernetes;

5.2.85 Deve suportar integração com Solução de SIEM multi fabricante;

5.2.86 Deve suportar o protocolo padrão da indústria VXLAN;

5.2.87 A solução deve suportar a integração nativa com soluções de sandboxing;

5.2.88 O appliance deve estar licenciado e permitir a utilização de no mínimo 9 (nove) instâncias virtuais;

5.2.89 Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

5.2.90 Reconhecer no mínimo 3000 aplicações diferentes, em camada 7, 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 e-mail;

5.2.91 Reconhecer no mínimo 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, activedirectory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

5.2.92 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;

5.2.93 Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

5.2.94 Identificar o uso de táticas evasivas via comunicações criptografadas;

5.2.95 Atualizar a base de assinaturas de aplicações automaticamente;

5.2.96 Limitar a banda (download/upload) usada por aplicações (trafficshaping), baseado no IP de origem, usuários e grupos;

5.2.97 Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

5.2.98 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;

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

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

5.2.101 Deve possibilitar a diferenciação de tráfegos de InstantMessaging (AIM, Hangouts,

Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;

5.2.102 Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;

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

5.2.104 Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, BrowseBased, Network Protocol, etc);

5.2.105 Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;

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

5.2.107 Deve ser possível configurar ApplicationOverride permitindo selecionar aplicações individualmente;

5.2.108 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;

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

5.2.110 As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

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

5.2.112 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;

5.2.113 Deve permitir o bloqueio de vulnerabilidades;

5.2.114 Deve incluir proteção contra ataques de negação de serviços;

5.2.115 Deverá possuir os seguintes mecanismos de inspeção de IPS: Análise de decodificação de protocolo, Análise para detecção de anomalias de protocolo, IP Defragmentation, Remontagem de pacotes de TCP, de pacotes mal formados e Bloqueio;

5.2.116 Ser imune e capaz de impedir ataques básicos como: Synflood, ICMP flood,

UDPflood, etc;

5.2.117 Detectar e bloquear a origem de portscans;

5.2.118 Bloquear ataques efetuados por worms conhecidos;

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

5.2.120 Possuir assinaturas para bloqueio de ataques de buffer overflow;

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

5.2.122 Identificar e bloquear comunicação com botnets;

5.2.123 Registrar na 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;

5.2.124 Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;

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

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

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

5.2.128 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 usuários, origem, destino e zonas de segurança;

5.2.129 Fornecer proteção contra ataques de dia zero por meio de estreita integração com os componentes incluindo NGFW (Next Generatil Firewall), Sandbox (on-premise ou nuvem);

5.2.130 Deve ser considerado para esta especificação proteção via Sandbox do fabricante do NGFW ou terceiros, na modalidade "in cloud" ou "on premisses", permitindo também na oferta de soluções on premisses, appliances físicos ou virtuais.

5.2.131 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);

5.2.132 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, em modo de proxy transparente e explícito;

5.2.133 Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

5.2.134 Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;

5.2.135 Possuir no mínimo 60 categorias de URLs;

5.2.136 Deve possuir a função de exclusão de URLs do bloqueio, por categoria;

5.2.137 Permitir a customização de página de bloqueio;

5.2.138 Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);

5.2.139 Além do Explicit Web Proxy, suportar proxy Web transparente;

5.2.140 Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;

5.2.141 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;

5.2.142 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 ou qualquer tipo de restrição de uso como, mas não limitado à utilização de sistemas virtuais, segmentos de rede, etc;

5.2.143 Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

5.2.144 Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

5.2.145 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);

5.2.146 Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

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

5.2.148 Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso à internet e gerenciamento da solução;

5.2.149 Com a finalidade de controlar aplicações de camada 7 e tráfego cujo consumo possa ser excessivo, (como Youtube, Ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esses tipos de aplicações, deve ter a capacidade de controlá-las por políticas de máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;

5.2.150 Suportar a criação de políticas de QoS e TrafficShaping por endereço de origem;

5.2.151 Suportar a criação de políticas de QoS e TrafficShaping por endereço de destino;

5.2.152 Suportar a criação de políticas de QoS e TrafficShaping por usuário e grupo;

5.2.153 Suportar a criação de políticas de QoS e TrafficShaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

5.2.154 Suportar a criação de políticas de QoS e TrafficShaping por porta;

5.2.155 O QoS deve possibilitar a definição de tráfego com banda garantida;

5.2.156 O QoS deve possibilitar a definição de tráfego com banda máxima;

5.2.157 O QoS deve possibilitar a definição de fila de prioridade;

5.2.158 Suportar marcação de pacotes Diffserv, inclusive por aplicação;

5.2.159 Suportar modificação de valores DSCP para o Diffserv;

5.2.160 Suportar priorização de tráfego usando informação de Typeof Service;

5.2.161 Deve suportar QoS (traffic-shapping), em interface agregadas ou redundantes;

5.2.162 Permitir a criação de filtros para arquivos e dados pré-definidos;

5.2.163 Os arquivos devem ser identificados por extensão e tipo;

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

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

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

5.2.167 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;

5.2.168 Deve contemplar a oferta do licenciamento de DLP caso a solução ofertada possua;

5.2.169 Suportar a criação de políticas por geolocalização, permitindo o trafego de determinado Pais/Países sejam bloqueados;

5.2.170 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

5.2.171 Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;

5.2.172 Permitir a utilização das funcionalidades de VPN Site-to-Site e Cliente-To-Site;

5.2.173 Permitir utilizar IPSec VPN sem limitação de licenciamento caso a solução ofertada possua;

5.2.174 Permitir utilizar SSL VPN sem limitação de licenciamento caso a solução ofertada possua;

5.2.175 A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;

5.2.176 A VPN IPSEc deve suportar Diffie-HellmanGroup 1, Group 2, Group 5 e Group 14;

5.2.177 A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

5.2.178 A VPN IPSEc deve suportar AES 128, 192 e 256 (AdvancedEncryption Standard);

5.2.179 Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

5.2.180 Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;

5.2.181 Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;

5.2.182 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;

5.2.183 Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

5.2.184 Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;

5.2.185 Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

5.2.186 Deverá manter uma conexão segura com o portal durante a sessão;

5.2.187 O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior).

5.2.188 Deverá suportar implementação de SD-WAN e possuir Console de Gerência Centralizada para essa solução;

5.2.189 A solução SD-WAN deve ser fornecida no mesmo appliance que o NGFW;

5.2.190 O SD-WAN deverá suportar vários links de acesso, como MPLS, Internet dedicada e Internet Móvel;

5.2.191 Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

5.2.192 Deve possuir capacidade de agregar e balancear, no mínimo, 2 circuitos de dados utilizando uma interface dedicada para cada circuito;

5.2.193 Deve permitir a configuração de ISP (rota default estática) com a utilização de probe ou de forma similar para verificar a disponibilidade do provedor. A probe ou similar deve permitir verificar o acesso HTTP a pelo menos 1 (um) site web e deve considerar o ISP indisponível em caso de falha (ou alta latência);

5.2.194 Deve balancear o tráfego das aplicações entre múltiplos links simultaneamente;

5.2.195 Deve realizar a redistribuição do balanceamento do tráfego entre os links de comunicação utilizados, em caso de falhas nesses links, ou de acordo com as políticas de qualidade pré-definidas;

5.2.196 Deverá simplificar a implantação de túneis criptografados de site para site;

5.2.197 Deverá implementar a PKI usando a autoridade de certificação (CA);

5.2.198 Deverá permitir a comunicação indireta entre localidades por meio de topologia “hub andspoke”;

5.2.199 Deverá balancear o tráfego das aplicações entre múltiplos links simultaneamente;

5.2.200 Deverá analisar o tráfego em tempo real e realizar o balanceamento dos pacotes de um mesmo fluxo entre múltiplos links simultaneamente em uma extremidade e realizar a reordenação dos pacotes desse mesmo fluxo no outro extremo;

5.2.201 Deverá monitorar a latência, o jitter e o descarte de pacotes em cada um dos links individualmente;

5.2.202 A Solução SD-WAN deve realizar a redistribuição do balanceamento do tráfego entre os links de comunicação utilizados pelos Gateways, em caso de falhas nesses links, ou de acordo com as políticas de qualidade pré-definidas;

5.2.203 Deverá suportar arquitetura VRF, onde o tráfego poderá ser segmentado com base em uma definição comum de VRFs em todos os sites;

5.2.204 Deverá possuir serviço de servidor DHCP;

5.2.205 Deverá possuir serviço de DHCP relay;

5.2.206 Deverá implementar rotas estáticas;

5.2.207 Deverá implementar OSPF;

5.2.208 Deverá implementar BGP;

5.2.209 Deve ser possível implementar SD-WAN em alta disponibilidade (pelo menos 2 appliances) na Câmara Municipal;

5.2.210 Deve ser possível implementar SD-WAN utilizando VRRP e realizar a recuperação de falhas através de um roteador compatível com esse protocolo;

5.2.211 Deverá suportar aplicativos hospedados em Data Center próprio e também aqueles consumidos como serviço na nuvem;

5.2.212 A solução deverá garantir performance de aplicações que utilizam VPN nos sites remotos e serviços de nuvem (SaaS);

5.2.213 A solução deverá medir e reagir independentemente à condição de rede UNIDIRECIONALMENTE para todas as condições (Latência, Jitter, Perda, Largura de banda - BW);

5.2.214 Deverá fornecer desempenho para os aplicativos em um cenário de link de transporte duplo quando um dos links está prejudicado;

5.2.215 Deverá fornecer desempenho para os aplicativos em um cenário de link de transporte duplo quando os dois links estão prejudicados;

5.2.216 A Solução deverá possuir algum mecanismo de QoS para proteger o tráfego de Internet quanto tiver congestionamento na unidade regional;

5.2.217 A Solução deverá permitir que sites de unidades regionais acessem sites VPN legados (não-SD-WAN) sem fazer backhauling do tráfego de aplicativos por meio de um hub SD-WAN;

5.2.218 Deve ser possível criar políticas para a modelagem do tráfego definindo pelo menos os parâmetros:

5.2.219 IP de Origem;

5.2.220 IP de Destino;

5.2.221 Porta TCP/UDP de Destino;

5.2.222 Domínio e URL de destino;

5.2.223 Aplicação de camada 7 utilizada (Office 365, Exchange, SAS, Dropbox, Box, Zoom e etc);

5.2.224 Agendamento e gerenciamento de filas;

5.2.225 Remarcação de DSCP;

5.2.226 Definição dos links utilizados em situação normal;

5.2.227 Definição dos links utilizados em caso de falha do(s) link(s) primários;

5.2.228 TrafficShapping;

5.2.229 A solução deverá suportar convergência rápida de tráfego de um túnel ao outro sem perda de sessões TCP/UDP previamente estabelecidas;

5.2.230 Poderá ser configurado utilizando perfis e políticas de segurança atribuídos de forma dinâmica;

5.2.231 Deverá possuir serviço de Firewall Stateful;

5.2.232 Deverá fornecer criptografia AES de 128 bits ou AES de 256 bits em sua VPN;

5.2.233 A solução deve permitir a inserção automática de serviços de segurança de nuvem, ou seja, com intercepção de tráfego por aplicação e envio à diferentes fornecedores de serviços de segurança em nuvem.

5.2.234 A solução deve suportar VPNs do tipo Hub Spoke e Full Mesh;

5.2.235 A solução deverá oferecer uma API RESTful completa para integração de orquestração no NOC de forma segura e criptografada;

5.2.236 Todo o provisionamento de serviços deverá ser feito via GUI no sistema de gerenciamento;

5.2.237 Todas as alterações de configuração deverão ser registradas e arquivadas para fins de auditoria;

5.2.238 Deverá suportar SNMP versões 2c e 3;

5.2.239 A console de Gerência deverá informar o status UP/DOWN/SPEED das interfaces LAN e WAN;

5.2.240 Deverá permitir que todos os alarmes e eventos sejam registrados na console de Gerência;

5.2.241 A Gerência SD-WAN deverá enviar mensagens syslog referentes aos Gateways SD-WAN para um servidor syslog externo da CONTRATADA e da CONTRATANTE;

5.2.242 Deverá realizar medições de latência, Jitter e descarte de pacotes para cada destino em cada uma das interfaces dos Gateways SD-WAN a cada 5 (cinco) minutos no mínimo;

5.2.243 As medições de taxa de ocupação do link, latência, Jitter e descarte de pacotes e as estatísticas de interface deverão ser coletadas de cada Gateway SDWAN a cada 5 (cinco) minutos no mínimo;

5.2.244 As medições de taxa de ocupação do link, latência, Jitter e descarte de pacotes deverão ser visíveis na GUI da gerência SD-WAN;

5.2.245 Possuir os contadores de estatísticas de LAN e WAN dos Gateway SD WAN (bits RX/TX, entrada/saída de pacotes, descartes de pacotes e erros);

5.2.246 Deverá ter a capacidade para medir os fluxos de aplicativos como volume de dados trafegados, quantidade de transações entre outros;

5.2.247 Os resultados de desempenho de link e aplicativo deverão ser visualizados em forma de gráfico a partir da GUI de Gerência SD-WAN;

5.2.248 Deverá suportar exportação de registros Netflow / IPFIX/ Netstream baseada em padrões;

5.2.249 Deverá possuir provisionamento do Zero Touch que deverá funcionar de tal forma que um CPE SD-WAN seja enviado diretamente do fornecedor de SD-WAN para uma instalação do cliente sem a necessidade de configuração prévia do CPE SD-WAN;

5.2.250 Deverá ter a flexibilidade para ser gerenciada pelo cliente e/ou gerenciada pelo parceiro.

5.2.251 Deverá possibilitar Geolocalização do dispositivo;

5.2.252 Deverá manter Backups de toda a solução sob sua guarda a fim de rápida recuperação em caso de substituição do equipamento.

5.3. Características Técnicas dos Serviços de Mapeamento de Vulnerabilidades:

5.3.1 Varredura simples para descobrir hosts ativos e portas abertas;

5.3.2 Varredura completa do sistema indicada para qualquer ativo na rede;

5.3.3 Verificação sem restrições ou recomendações;

5.3.4 Verificação dinâmica de plug-in sem restrições ou recomendações;

5.3.5 Verificação de malware em sistema Windows e Unix;

5.3.6 Verificação de vulnerabilidades da Web publicadas e desconhecidas;

5.3.7 Verificação de autenticação para hospedagem e enumeração de atualizações ausentes;

5.3.8 Verificações remotas e locais para CVE-2017-5689;

5.3.9 Verificação remota e local para CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754;

5.3.10 Verificação remota e local para MS17-010;

5.3.11 Varredura remota para hosts de impressão digital potencialmente executando a pilha Treck na rede;

5.3.12 Verificação remota para detectar a elevação de privilégio do Microsoft Netlogon (zerologon);

5.3.13 Verificação local e remota para detectar vulnerabilidades do SolarWindsSolorigate;

5.3.14 Verificação local e remota para detectar vulnerabilidades do Exchange direcionadas pelo HAFNIUM;

5.3.15 Verificação local para detectar a vulnerabilidade do PrintNightmare no spooler de impressão do Windows;

5.3.16 Busque por configurações incorretas no Active Directory;

5.3.17 Detecção do Apache Log4j CVE-2021-44228;

5.3.18 Detecção do Apache Log4j CVE-2021-44228 por meio de verificações diretas;

5.3.19 Detecção de vulnerabilidades do Log4Shell;

5.3.20 Detecção de vulnerabilidades de alertas recentes no CISA;

5.3.21 Detecção de vulnerabilidades de alertas recentes no CISA;

5.3.22 Auditoria de configurações de serviços de nuvem de terceiros;

5.3.23 Possibilitar verificação de vulnerabilidade interna do PCI DSS (11.21);

5.3.24 Possibilitar auditoria de configuração dos dispositivos de rede;

5.3.25 Possibilitar auditoria das configurações dos sistemas relacionadas a uma linha de base conhecida;

5.3.26 Possibilitar auditoria de sistemas utilizando definições SCAP e OVAL;

5.3.27 Deve possibilitar automatizar avaliações para encontrar, prever, avaliar, diagnosticar e apontar ações que devem ser realizadas para corrigir as vulnerabilidades encontradas;

5.3.28 Deve contemplar o recurso de Descobertas como a primeira etapa da avaliação de vulnerabilidades, gerando inventário completo de todos os ativos de rede, num ambiente distribuído. O processo de descoberta deve utilizar de recursos de avaliação de vulnerabilidades com softwares dotados de inteligência artificial devidamente licenciado;

5.3.29 Deve contemplar o recurso de Avaliar para identificar de forma rápida e eficiente as vulnerabilidades, as configurações incorretas, os pontos fracos na rede de computadores, ativos e vetores de ameaças em potencial;

5.3.30 Deverá contemplar o recurso de Conformidade, neste processo é realizado uma auditoria nas conformidades das configurações, embasadas na análise de benchmarks do Center for Internet Security (CIS) e conjunto de melhores práticas compiladas nas áreas de defesa, energia, finanças, transportes, engenharia etc;

5.3.31 Deverá contemplar o recurso de Analisar, esse recurso fornece visão geral da organização, analisará filtragens e agrupamentos sofisticados permitindo uma busca

detalhada com análise de resultados, para obter os detalhes de vulnerabilidades e o que podem ser potencialmente afetados acelerando o tempo de detecção, análise e correção;

5.3.32 Deverá contemplar o recurso de Relatar no formato PDF todos os snapshots e informações colhidas no processo de mapeamento de vulnerabilidades, informando as características da análise.

5.3.33 O mapeamento de vulnerabilidades deverá ser realizado, após a implementação das soluções de NGFW, como condição de entrega e validação destes serviços;

5.3.34 O processo de mapeamento de vulnerabilidades deverá ser realizado por técnicos da CONTRATADA devidamente capacitado;

5.3.35 Deverá ser enviado no prazo máximo de 10 dias úteis após a realização de cada mapeamento de vulnerabilidades, relatório detalhado com resultados da análise, para um e-mail indicado pela CONTRATANTE.

5.4. <u>Características Técnicas dos Serviços de Captive Portal:</u>

5.4.1 Possuir controle de banda por usuário;

5.4.2 Possuir tempo de acesso do usuário;

5.4.3 Possuir horários de acesso do usuário;

5.4.4 Possuir logs de acesso do usuário;

5.4.5 Possuir acesso painel gerenciador via Cloud;

5.4.6 Possuir login automático por MAC (sem a necessidade de autenticação);

5.4.7 Possibilitar bloqueio de sites;

5.4.8 Possibilitar bloqueio P2P;

5.4.9 Possuir painel “Dashboard Admin” com especificações de gestão centralizada em nuvem contendo acessos de todas as unidades públicas municipais;

5.4.10 Possuir gráfico contendo com informações do comportamento da conexão;

5.4.11 Possuir gráfico de cadastro por tipo de autenticação;

5.4.12 Possuir painel com o recorde dos acessos;

5.4.13 Informar o número de checkins na plataforma;

5.4.14 Possuir informações demográficas (logins realizados via mídias sociais);

5.4.15 Informar a tecnologia utilizada pelo usuário (android/IOS);

5.4.16 Possibilitar cadastro manual de usuários no painel;

5.4.17 Possuir filtros de consulta de usuários;

5.4.18 Possibilitar cadastro com observações;

5.4.19 Possibilitar cadastro de usuários com informações de login;

5.4.20 Possibilitar cadastro de usuário com dados avançados contendo endereço MAC atual, USERNAME, MAC utilizados, total de DOWNLOAD (consumo), total de UPLOAD (consumo), número de conexões com data e hora do acesso;

5.4.21 Possibilitar a criação de grupos com perfis de acesso para alocação de clientes específicos;

5.4.22 Possibilitar habilitar alertas ou não de quando um usuário específico se conectar;

5.4.23 Possibilitar gerar relatórios com dados de consumo de banda por usuário;

5.4.24 Possibilitar a criação de vouchers de acesso;

5.4.25 Possibilitar a realizar sorteios de vouchers;

5.4.26 Permitir personalizar tela de login – logo;

5.4.27 Permitir personalizar tela de login - título da página;

5.4.28 Permitir personalizar tela de login - cor topo e botões de ação;

5.4.29 Permitir personalizar tela de login - cor de fundo;

5.4.30 Permitir personalizar tela de login – cor de texto;

5.4.31 Possibilitar limitação de download e upload;

5.4.32 Possibilitar autenticação por Facebook, Linkedin, Twitter, Email, SMS, Registro Direto, Código de liberação, Usuário e senha (cadastro manual) e Voucher de Acesso;

5.4.33 Possibilitar a criação de QrCode para acesso;

5.4.34 Possuir botão para cadastrar termo de uso personalizado de acordo com políticas internas do SAMAE;

5.4.35 Possibilitar a criação de diferentes perfis de acesso com as configurações de nome do perfil, descrição do perfil em texto livre, login automático do usuário, tempo máximo de sessão em minutos, tempo máximo ocioso em minutos e tempo máximo diário em minutos.

5.4.36 Os serviços de captive portal devem ser configurados no momento da implantação da solução de NGFW;

5.4.37 Aderente ao Marco Civil da Internet (Devendo registrar o horário, MAC Address e IP dos equipamentos conectados e armazenar histórico de acesso);

5.4.38 Aderente a LGPD com a possibilidade de opção de criação de termo de uso personalizado, página para gestão de informações do usuário e habilitação do aceite ao termo de uso como obrigatório para login;

5.4.39 Logar e armazenar em nuvem própria por no mínimo 180 dias e 100% dos acessos da solução;

5.4.40 Deverá ser fornecido no mínimo 200 acessos simultâneos Wi-Fi via redes sociais ou e-mail, para cada equipamento NGFW;

5.4.41 A solução deverá se integrar sem nenhum hardware ou software adicional ao dispositivo NGFW;

5.4.42 Não contempla fornecimento de Acces Point neste serviço;

5.4.43 Não contempla configuração de Access Point neste serviço;

5.4.44 Permitir integração com a solução ofertada;

5.4.45 É de responsabilidade da CONTRATANTE toda a gestão de acesso aos serviços de Captive Portal;

5.4.46 Deverá ser fornecido treinamento On-Site, com carga horária de 4 horas para no mínimo 2 técnicos da CONTRATANTE.

5.5. Características Técnicas da Solução da Base de Dados Analíticos e Logs:

5.5.1 A solução de base de dados Analíticos e Log deverá ser fornecida em Virtual Machine ou Nuvem da CONTRATADA e ser do mesmo fabricante da solução NGFW;

5.5.2 Deve suportar o acesso via SSH, WEB (HTTPS) para gerenciamento da solução;

5.5.3 Possuir comunicação e autenticação criptografada com usuário e senha para obter relatórios, na interface gráfica (GUI) e via linha de comando no console de gerenciamento;

5.5.4 Deve possuir a capacidade de armazenar de forma centralizada no mínimo 30 Gigas de Log/Dia por dispositivo NGFW, por período mínimo de 90 dias;

5.5.5 Deve possuir capacidade de gerenciar Logs de no mínimo 2 dispositivos do tipo NGFW;

5.5.6 A solução deve ter o recurso de Multi-tenancy, possibilitando separar os logs de NGFW por grupos de acessos;

5.5.7 Permitir acesso simultâneo à administração, bem como criar no mínimo 2 (dois) perfis para administração e monitoramento;

5.5.8 Possuir suporte para SNMP versão 2 e 3;

5.5.9 Permitir a virtualização do gerenciamento e administração dos dispositivos, onde cada administrador tem acesso apenas aos equipamentos autorizados;

5.5.10 Deve permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução;

5.5.11 Deve estar licenciado, permitindo o uso integrado e operacional de todas as instâncias virtuais NGFW requisitadas;

5.5.12 Deve permitir ativar e desativar para cada interface da plataforma, as permissões de acesso HTTP, HTTPS e SSH;

5.5.13 Permitir a autenticação de usuários de acesso à plataforma via LDAP;

5.5.14 Permitir a autenticação de usuários de acesso à plataforma via Radius;

5.5.15 Permitir a autenticação de usuários de acesso à plataforma via TACACS +;

5.5.16 Permitir a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;

5.5.17 Permitir a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;

5.5.18 Permitir a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;

5.5.19 Permitir a definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais;

5.5.20 Deve conter um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha;

5.5.21Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;

5.5.22 Deve possuir mecanismos de remoção automática para logs antigos;

5.5.23 Permitir importação e exportação de relatórios;

5.5.24 Deve ter a capacidade de criar relatórios no formato HTML;

5.5.25 Deve ter a capacidade de criar relatórios em formato PDF;

5.5.26 Deve ter a capacidade de criar relatórios no formato XML;

5.5.27 Deve ter a capacidade de criar relatórios no formato CSV;

5.5.28 Deve permitir exportar os logs no formato CSV;

5.5.29 Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;

5.5.30 Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;

5.5.31 A solução deve ter relatórios predefinidos;

5.5.32 Deve permitir o envio automático dos logs para um servidor FTP externo a solução;

5.5.33 A duplicação de relatórios existentes deve ser possível para edição posterior;

5.5.34 Deve ter a capacidade de personalizar a capa dos relatórios obtidos;

5.5.35 Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs;

5.5.36 Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;

5.5.37 Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;

5.5.38 Deve ter um mecanismo de "pesquisa detalhada" ou "Drill-Down" para navegar pelos relatórios em tempo real;

5.5.39 Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;

5.5.40 Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;

5.5.41 Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;

5.5.42 Permitir o envio de relatórios por e-mail automaticamente;

5.5.43 Deve permitir que o relatório seja enviado por e-mail para o destinatário específico;

5.5.44 Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;

5.5.45 Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado;

5.5.46 Deve permitir o uso de filtros nos relatórios;

5.5.47 Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;

5.5.48 Permitir especificar o idioma dos relatórios criados;

5.5.49 Gerar alertas automáticos via e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;

5.5.50 Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;

5.5.51 Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;

5.5.52 Possibilidade de exibir nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;

5.5.53 Deve ter uma ferramenta que permita analisar o desempenho na geração de relatórios, com o objetivo de detectar e corrigir problemas na geração deles;

5.5.54 A solução deve permitir importar arquivos com logs de dispositivos compatíveis conhecidos e não conhecidos pela plataforma, para geração posterior de relatórios;

5.5.55 Deve ser possível definir o espaço que cada instância de virtualização pode usar para armazenamento de log;

5.5.56 Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;

5.5.57 Deve ser compatível com a autenticação de fator duplo (token) para usuários do administrador da plataforma;

5.5.58 Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;

5.5.59 Deve permitir visualizar em tempo real os logs recebidos;

5.5.60 Deve permitir o encaminhamento de log no formato syslog;

5.5.61 Deve permitir o encaminhamento de log no formato CEF (Common Event Format);

5.5.62 Deve permitir gerar alertas de eventos a partir de logs recebidos;

5.5.63 Deve permitir a criação de incidentes a partir de alertas de eventos para o terminal;

5.5.64 Deve permitir a integração ao sistema de tickets do ServiceNow;

5.5.65 Deve possuir o serviço de Indicadores de Compromisso (IoC) do mesmo fabricante, que mostra as suspeitas de envolvimento do usuário final na Web e deve relatar pelo menos: endereço IP do usuário, nome do host, sistema operacional, veredito (classificação geral da ameaça) e o número de ameaças detectadas;

5.5.66 Deve possuir o serviço de detecção de surtos (Outbreak) com detecção automatizado de novos malwares, incluindo relatório resumo de como o malware detectado age;

5.5.67 Deve suportar o padrão SAML para autenticação do usuário administrador;

5.5.68 Deve ter um relatório de uso do aplicativo SaaS;

5.5.69 Deve ter um relatório de prevenção de perda de dados (DLP);

5.5.70 Deve ter um relatório de VPN;

5.5.71 Deve ter um relatório IPS (IntruderPrevention System);

5.5.72 Deve ter um relatório de reputação do cliente;

5.5.73 Deve ter um relatório de análise de segurança do usuário;

5.5.74 Deve ter um relatório de análise de ameaças cibernéticas;

5.5.75 Deve ter um relatório diário resumido de eventos e incidentes de segurança;

5.5.76 Deve ter um relatório de tráfego DNS;

5.5.77 Deve ter um relatório de tráfego de e-mail;

5.5.78 Deve ter um relatório dos 10 principais aplicativos usados na rede;

5.5.79 Deve ter um relatório dos 10 principais sites usados na rede;

5.5.80 Deve ter um relatório de uso de mídia social.

5.6. Características Técnicas do Controlador de Usuários (Microsoft Active Directory – AD) Licenciado:

Em razão dos sistemas operacionais da Câmara Municipal de SINOP serem todos Windows, necessariamente o controlador de usuários a serem fornecidos é o Microsoft Active Directory (AD), o qual deve ser fornecido 1 (uma) licença instalada e configurada, para propiciar a entrega e ter as seguintes funcionalidades:

5.6.1 O controlador de usuários deverá ser instalado e licenciado em servidor físico ou virtual fornecido pela CONTRATANTE;

5.6.2 É de total responsabilidade da CONTRATANTE realizar os cadastros dos usuários no controlador de usuários, ficando a CONTRATADA responsável por criar a estrutura de UNIDADES ORGANIZACIONAIS, GRUPOS DE USUÁRIOS e INTEGRAÇÕES necessárias para a Câmara Municipal de Sorriso;

5.6.3 É de total responsabilidade da CONTRATANTE ingressar os servidores, desktops, notebooks, etc ao controlador de usuários, ficando a CONTRATADA responsável pelo suporte técnico e repasse de conhecimento para o técnico da Câmara Municipal;

5.6.4 Armazenamento de Dados: O AD deve armazenar informações sobre usuários, grupos, computadores, senhas e outras contas de rede;

5.6.5 A gerência do controlador de usuários é de responsabilidade da CONTRATANTE, inclusive a política de senhas, tempo de troca e acesso ao controlador;

5.6.6 Para o controlador de usuários deve ser fornecido licenciamento do Microsoft Windows Server versão mínima 2019;

5.6.7 O controlador deve autenticar e verificar a identidade dos usuários ao fazer login, garantindo que apenas usuários autorizados possam acessar recursos da rede;

5.6.8 O controlador deve autorizar e controlar quais usuários têm permissão para acessar determinados recursos na rede;

5.6.9 O controlador deve replicar os dados de usuários do diretório por meio de uma rede, garantindo que todas as cópias dos dados estejam atualizadas;

5.6.10 Deve permitir administração centralizada e facilitada a administração de usuários e recursos de rede, permitindo políticas de segurança e configurações centralizadas;

5.6.11 O controlador de usuários deve ser organizado de forma hierárquica, com domínios

que atuam como limites administrativos e de segurança. Isso permite que diferentes domínios tenham diferentes administradores e políticas de segurança;

5.6.12 Com o objetivo de facilitar a segurança, devem ser criadas Unidades Organizacionais e Grupos separados para fins de gerenciamento de acesso a pastas e arquivos separados das permissões de acesso a sites e aplicações web.

5.7. Características Técnicas da Solução de plataforma de conscientização em proteção de dados:

5.7.1 A CONTRATADA deverá fornecer os seguintes serviços para atendimento desta solução:

a) Subscrição de licença de plataforma integrada de campanhas de phishing e treinamentos on-line, na modalidade de Ensino à Distância (EaD), voltados à capacitação e conscientização em Segurança da Informação, Segurança Cibernética e Proteção de Dados Pessoais. Licença para 12 meses com quantidade de 100 licenças

b) Suporte técnico especializado para a plataforma integrada de campanhas de phishing e treinamentos online. Suporte para 12 meses com no mínimo 20 horas

c) Treinamento para administração da plataforma (on-line). Suporte para 3 horas com no mínimo 5 horas.

5.7.2. Os serviços devem compreender o seguinte:

5.7.2.1 Identificar usuários que necessitam de treinamento em Segurança da Informação, Segurança Cibernética e Proteção de Dados Pessoais, através de campanhas de phishing;

5.7.2.2 Gerar estatísticas de uso para identificar elementos que possam confundir o usuário a clicar em links maliciosos ou responder a e-mails de phishing;

5.7.2.3 Consolidar os dados coletados para permitir a análise crítica e a avaliação de ações pela Administração, mitigando riscos relacionados à utilização do e-mail corporativo;

5.7.2.4 Proporcionar ferramentas e recursos educacionais para capacitar os usuários conforme suas necessidades individuais.

5.7.3 O objetivo da contratação da plataforma integrada de campanhas de phishing e treinamentos on-line é para gerar os seguintes benefícios:

5.7.3.1 Aumento da conscientização sobre as melhores práticas de segurança dainformação;

5.7.3.2 Melhoria na compreensão dos riscos e ameaças cibernéticas;

5.7.3.3 Fortalecimento das habilidades em identificar e reportar incidentes de segurança;

5.7.3.4 Redução do número de incidentes de segurança causados por erros humanos;

5.7.3.5 Aumento da adesão às políticas e diretrizes de segurança da informação;

5.7.3.6 Melhoria na proteção dos dados pessoais e informações sensíveis da Câmara Municipal de Sinop;

5.7.3.7 Criação de uma cultura de segurança da informação, tornando-se agentes naproteção de ativos e recursos digitais desta instituição.

5.7.4 A CONTRATADA deve realizar um treinamento para a equipe da CONTRATANTE que atuará com a administração da plataforma integrada de campanhas de phishing e treinamentos on-line;

5.7.5 A capacitação da equipe técnica designada pela CONTRATANTE poderá ser realizada presencialmente, em suas instalações, ou por meio de Ensino à Distância (EaD) síncrono (on-line e ao vivo), com a opção de gravação ser disponibilizada posteriormente à CONTRATANTE;

5.7.6 A capacitação deve abranger a gestão e operação da plataforma, ocorrendo preferencialmente nos primeiros dias úteis após a assinatura do contrato;

5.7.7 Para a capacitação técnica exigida para este item, nos termos do art. 67 da Lei n.º 14.133/2021, a LICITANTE deverá apresentar atestado/declaração de capacidade técnica fornecido por pessoas jurídicas de direito público ou privado, cujo quantitativo total atestado deve comprovar o fornecimento de licenças e a prestação de serviço de suporte técnico, correspondendo a pelo menos 50% das quantidades descritas no objeto deste Termo de Referência;

5.7.8 Caso a LICITANTE não seja o fabricante dos produtos ou serviços, deve comprovar, juntamente com a proposta de preços para o presente certame, ser uma revenda ou prestadora de serviços autorizada, assegurando a propriedade intelectual do fabricante relativa aos direitos autorais sobre as atualizações de softwares e serviços de suporte ofertados.

5.8. Características Técnicas da Solução de Backup em Nuvem:

5.8.1 Deve possibilitar backups em nível de arquivo, em nível de disco, de imagem e de aplicativo;

5.8.2 O gerenciamento da solução ofertada deverá ser via interface WEB (HTTPS);

5.8.3 Deve possibilitar realizar backups de workloads populares, como as de Mac, Windows, Linux, Microsoft 365, Google Workspace, Hyper-V e Vmware;

5.8.4 Deve possibilitar opções híbridas de armazenamento – armazenamento em nuvem, nuvens públicas (como Microsoft Azure, AWS e Google Cloud) ou armazenamento local do

MSP;

5.8.5 Deve possuir opções de recuperação flexíveis, desde sistemas completosaté arquivos granulares;

5.8.6 Deve possibilitar migração entre nuvem, local e virtual;

5.8.7 Deve possuir antimalware e antivírus baseados em inteligência de máquina para combater ameaças de dia zero e ransomware;

5.8.8 Deve possuir criptografia do arquivamento;

5.8.9 Deve possibilitar backups incrementais e diferenciais;

5.8.10 Deve possibilitar backups imutáveis;

5.8.11 Deve possibilitar avaliações de vulnerabilidades;

5.8.12 Deve possuir proteção completa para Google Workspace;

5.8.13 Deve possuir proteção completa para o Microsoft 365;

5.8.14 Deve possuir criptografia de backups;

5.8.15 Deve possuir eliminação de duplicidade;

5.8.16 Deve possuir monitoramento e geração de relatórios;

5.8.17 Deve possuir proteção de dados continuada objetivando somente backups das alterações em tempo real, assegurando que nenhum dado seja perdido;

5.8.18 Deve possibilitar compatibilidade de backup expandida abrangendo clusters de Microsoft SQL, clusters de Microsoft Exchange, MariaDB, MySQL, Oracle DB e SAP HANA;

5.8.19 Deve possibilitar mapa de proteção de dados e relatórios de conformidade que examine os ambientes para assegurar workloads, arquivos, aplicativos e usuários;

5.8.20 Deve possibilitar processamento de dados fora do host: mova tarefas de backup para uma outra máquina, na forma de operações de máquina virtual, para reduzir a carga sobre as workloads do cliente;

5.8.21 Deve possibilitar a realização de no mínimo 5 TB de backup de dados;

5.8.22 Deve possibilitar a realização de no mínimo Backup de 3 VM (virtual machine) com tamanho médio de 120 GB;

5.8.23 Deve possibilitar a funcionalidade de recuperação de desastres (DR), permitindo restaurar a VM e subir os serviços da mesma estrutura;

5.8.24 Deve permitir para os casos de utilização dos serviços de DR tempo máximo de produção das 3 VM’s de 504 horas anual;

5.8.25 É de total responsabilidade da CONTRATADA manter os serviços ofertados com

suporte técnico 24x7;

5.8.26 Deverá ser fornecido pela CONTRATADA treinamento de no mínimo 3 horas para os técnicos da CONTRATANTE.

5.9. Especificações Técnicas Gerais:

a) A CONTRATADA deverá garantir a prestação dos serviços, conforme as exigências e determinações constantes neste instrumento, independentemente de marca e modelos dos produtos, software ou hardwares que serão utilizados;

b) Cada hardware deverá ser fornecido com todos os acessórios e programas necessários à sua instalação, operação e monitoração, cabendo inclusive, a CONTRATADA, a instalação do hardware e configurações de todas as funcionalidades da solução;

c) Toda a solução deve ser nova, disponível para primeiro uso e em pleno período de vida, sem previsão de término dos tempos de vida, vendas e suporte;

d) Não serão aceitos equipamentos em modo End of Support, End of Life ou equivalentes anunciados pelo fabricante até a data da abertura das propostas que englobem o período total do contrato. Dessa forma, na data de abertura das propostas, o equipamento deveestar em sua fase do ciclo de vida de plena comercialização e suporte, não sendo aceitos equipamentos com qualquer limitação a essa condição (End of Life, End of Support ou equivalente) considerando a data de abertura das propostas, essa condição será verificada por meio do acesso ao site do fabricante;

e) Toda a solução de segurança NGFW deverá ser entregue em hardware dedicado do tipo appliance do mesmo fabricante;

f) A solução de base de dados Analíticos e Log deverá ser fornecida em Virtual Machine ou Nuvem da CONTRATADA e ser do mesmo fabricante da solução NGFW;

g) Toda a solução deve ser fornecida contemplando garantia do fabricante, durante toda a vigência do contrato;

h) Todos os equipamentos NGFW que compõem a solução devem possuir homologação da Agência Nacional de Telecomunicações (ANATEL), conforme determina a Resolução nº 715, de 23 de outubro de 2019, com validade na data da apresentação das propostas. Os documentos comprobatórios deverão ser apresentados juntamente com a proposta comercial;

i) Deverá ser disponibilizado até 2 (duas) horas de treinamento e campanhas educativas, presencial ou remota, em segurança da informação para os gestores e/ou grupos de servidores, através de profissional devidamente especializado em governança e segurança da

informação, conforme critérios a serem estabelecidos por este órgão;

j) Deverá ser elaborado um High-Level Design (HLD), contemplando todas as unidades públicas municipais com o detalhamento de como a solução ofertada atende às necessidades apontadas na licitação;

k) A aprovação do HLD deverá ser feita pela equipe técnica indicada pelo departamento de T.I do órgão;

l) Deverá ser apresentado um teste de laboratório (Nacional ou Internacional) que compare o produto ofertado com no mínimo 3 (três) fabricantes, garantindo que o equipamento seja capaz de:

- Prevenir no mínimo 70% (setenta por cento) dos malwares testados;
- Prevenir no mínimo 70% (setenta por cento) de variantes de malwares conhecidos;
- Possuir uma taxa de falso positivo na detecção de malware menor que 1% (um por cento);
- Possuir taxa de prevenção de phishing e URL maliciosas maior que 90% (noventa por cento);
- O teste deve ter duração mínima de 90 (noventa) dias com no mínimo 300 (trezentos) conjuntos de dados maliciosos (vírus e malwares).

m) Para o teste especificado acima, poderá ser utilizado como referência os testes realizados pela empresa Miercom (www.miercom.com). Um exemplo de teste que aborda todos os indicadores acima é o de número SR220915Q - NGFW Firewall Security Benchmark 2023 ou anos posteriroes - Firewall Security Efficacy Competitive Assessment Summary Lab Report;

n) O fabricante da solução de segurança ofertada deverá ser parceiro do site www.cve.org, onde deverão estar indicados todos os CVE (Common Vulnerabilities and Exposures);

o) O fabricante da solução de segurança ofertada deverá manter em seu site todos os CVE identificados, seu detalhamento e correções disponibilizadas.

5.10. Suporte Técnico:

a) Toda a solução deve ser fornecida contemplando suporte técnico 24x7 do Fabricante e da CONTRATADA;

b) A contratada deverá manter contrato de manutenção e de suporte de todos os ativos e seus respectivos softwares junto ao fabricante durante toda a vigência do contrato;

c) Deve ser contemplado e declarado em proposta o serviço de Suporte técnico que atenda os seguintes SLAs:

- Prazo máximo de reposta ao atendimento inicial em casos emergenciais com indisponibilidade de serviços em até 10 (dez) minutos;
- Prazo máximo de resposta ao atendimento inicial em casos com criticidade alta (situações de perda de funcionalidades ou instabilidades) em até 10 (dez) minutos;
- Prazo máximo para atendimento dos chamados em casos emergenciais com indisponibilidade de serviços de 1 (uma) hora;
- Prazo máximo para atendimento dos chamados com criticidade alta de 1 (uma) horas;
- Prazo máximo para atendimento dos chamados para solução de contorno em casos emergenciais com indisponibilidade dos serviços de até 3 (três) horas;

d) A CONTRATADA deverá disponibilizar técnicos especializados com disponibilidade 24x7 durante toda a vigência do contrato;

e) A CONTRATADA deverá demonstrar que possui número de telefone 0800, além de plataforma de atendimento para abertura de chamados de suporte técnico, o registro do atendimento é de total responsabilidade da CONTRATADA;

f) A CONTRATADA deve disponibilizar uma equipe especializada em monitoramento, detecção e mitigação de ataques, com opção de atendimento em idioma português, através de telefone 0800, correio eletrônico e whastApp ou Telegram, durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual, cujas informações devem estar indicadas na proposta comercial;

5.11 Qualificação Técnica

5.11.1 Comprovação de aptidão da contratada para o fornecimento de bens em características, quantidades e prazos compatíveis com o objeto da licitação, por meio da apresentação de atestados de capacidade fornecidos por pessoas jurídicas de direito público ou privado;

5.11.2 Para fins da comprovação de que trata este subitem, os atestados deverão ser compatíveis com o objeto deste Termo de Referência, especialmente, a respeito dos itens: 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9 e 5.10;

5.11.3 O atestado deverá comprovar o cumprimento dos requisitos técnicos para atendimento da solução ofertada, conforme especificações constantes neste Termo de Referência;

5.11.4 Os quantitativos dos atestados, mesmo que somados, devem comprovar a quantidade de no mínimo 50% dos itens especificados;

5.11.5 Demonstrar que possui em seu quadro de funcionários ou prestadores de serviços, como requisito de habilitação de participação no certame, profissional devidamente habilitado, para

prestar os serviços do objeto, considerando-se o seguinte:

5.11.5.1 No mínimo, 1 (um) engenheiro credenciado no órgão competente (CREA) como requisito de habilitação técnica, na data da realização do certame para apresentação de propostas vinculadas no **item 01;**

5.11.5.2 No mínimo, 2 (dois) profissionais técnicos em cibersegurança, sendo 1 (um) com certificação de nível profissional e outro com certificação de nível especialista da solução de segurança ofertada, sendo necessária a apresentação de documentação que comprove a validade desta(s) certificação(ões), como requisito de habilitação técnica, na data da realização do certame para apresentação de propostas vinculadas no **item 01;**

5.11.5.2.1 As certificações devem ser na área de Network Security e Security Operation;

5.11.6 No mínimo, 2 (dois) profissionais técnicos, com formação superior em Redes de Computadores, ou Ciência da Computação, ou assemelhados vinculados no **item 01 e 02**;

5.11.7 No mínimo, 1 (um) profissional em Gestão de Projeto, com graduação na área de Tecnologia da Informação, acompanhado de certificação PMP do PMI, em razão da complexidade do objeto licitado, a empresa CONTRATADA deverá indicar, como requisito de habilitação de participação no certame vinculadas no **item 01 e 02;**

5.11.8. Os profissionais acima relacionados deverão possuir vínculo com a empresa a ser Contratada cuja comprovação deverá ocorrer mediante apresentação de um dos documentos abaixo:

5.11.8.1. Apresentar cópia do registro na Carteira de Trabalho e Previdência Social – CTPS comprovando o vínculo empregatício do profissional na empresa licitante, ou Cópia de Contrato de Prestação de Serviços com firma reconhecida em cartório/ou assinada digitalmente de ambas as partes no caso de profissionais autônomos.

5.11.9 A CONTRATADA deverá demonstrar no ato de habilitação no certame, que possui a implantação aos termos da Lei Geral de Proteção de Dados, cuja demonstração deverá ocorrer na habilitação ao certame, com a apresentação de documentos que evidenciam a implementação, incluindo, mas não se limitando ao seguinte: Política de Privacidade, Política de Segurança da Informação, Registro de Atividades de Tratamento (RoPA) e Relatório de Medidas de Segurança;

5.11.10 A CONTRATADA deverá demonstrar que possui implementado ou que estejá em processo de adaptação às normas de ESG (Environmental, Social and Governance - Ambiental, Social e Governança), como requisito de habilitação no certame;

5.11.11 A contratada poderá realizar vistoria in loco para a verificação da infraestrutura atual

da CONTRATANTE, mediante prévio agendamento, com o departamento competente do órgão licitante, o qual deve emitir comprovante de realização desta vistoria, com data anterior à prevista para início do certame;

5.11.12 Caso a empresa não participe da visita técnica, deverá apresentar em substituição ao atestado de visita, declaração formal assinada pelo responsável técnico, sob as penalidades da lei, de que tem pleno conhecimento das condições e peculiaridades inerentes à natureza dos trabalhos, que assume total responsabilidade por esse fato e que não utilizará deste para quaisquer questionamentos futuros, avenças técnicas e financeiras;

5.11.13 Como requisito de aceite da Proposta de Preço no certame, em atendimento ao interesse da Administração, fica a cargo da equipe técnica de acompanhamento da licitação a possibilidade de solicitar complementação da documentação de comprovação técnica, ou a aprovação da mesma em caso de não atendimento de algum item do Demonstrativo de Comprovação das Especificações.

6 – EXECUÇÃO DO OBJETO DO CONTRATO

6.1. Local da Entrega dos Produtos e a Execução dos Serviços:

6.1.1. Os serviços deverão ser realizados na sede CMS, no setor do CPD, para análise do responsável técnico, o qual indicará onde serão feitas todas as instalações.

6.1.2. O prazo de entrega deverá ser de até 30 (Trinta) dias, de segunda a sexta feira, das 07:00 às 13:00 horas, a contar do recebimento da Nota de Autorização de Despesa ao responsável da empresa vencedora do certame licitatório, estando sujeitos à conferência e aceite pelo servidor responsável.

6.1.3. A(s) licitante(s) vencedora(s) se obriga(m) a entregar os serviços objetos desta licitação, mediante a emissão de ordem de fornecimento pela CMS, a partir da data da assinatura do Contrato, devendo os serviços obedecer a todas as normas técnicas e exigências inerentes aos mesmos.

6.1.4. Os serviços estarão sujeitos à conferência e aceite por funcionário responsável. Os serviços em desconformidade com as especificações contidas neste Termo de Referência serão rejeitados no ato da entrega pelo funcionário responsável, devendo a empresa sanar o problema em até 02 (dois) dias, sob pena de cancelamento da compra.

6.1.5. Caso a entrega do produto não possa ser realizada no prazo previsto, a empresa vencedora deverá fornecer documento justificativo em até 24 horas, para análise da Câmara Municipal que tomará as providências necessárias para adequação do fornecimento.

6.1.6. As notas fiscais não poderão ter rasuras e deverão descrever corretamente o item, e número de empenho, o número do processo de compras, dados bancários para depósito. As notas fiscais serão liberadas para pagamento somente quando atestadas o recebimento, ou seja, devidamente assinado e carimbado o recebimento dos materiais pelo funcionário responsável.

6.2 Obrigações das partes

6.2.1 Obrigações da CONTRATADA

6.2.1.1 Arcar com toda e qualquer despesa relativa ao fornecimento ora pactuado, dentre elas, carga, transporte, descarga, frete, impostos, mão-de-obra, taxas, contribuições, encargos sociais, inclusive nos casos de troca de item ou qualquer eventualidade que possa ocorrer.

6.2.1.2. Responsabilizar-se por todo e qualquer dano e/ou prejuízo que, eventualmente, venha a sofrer os objetos deste contrato, em decorrência do transporte dos mesmos.

6.2.1.3. As notas fiscais não poderão ter rasuras e deverão descrever corretamente o item, e número de empenho, o número do processo de compras, dados bancários para depósito.

6.2.1.4. Executar nas especificações e com a qualidade exigida.

6.2.1.5. Pagar todos os tributos, despesas e custos que incidam ou venham a incidir, direta ou indiretamente, sobre os produtos fornecidos.

6.2.1.6. Manter, durante a validade da Ata, as mesmas condições de habilitação.

6.2.1.7. Fornecer os produtos e serviços, no preço, prazo e forma estipulada na proposta.

6.2.2 Obrigações da CONTRATANTE

6.2.2.1 Atestar nas notas fiscais e/ou faturas a efetiva entrega dos materiais objeto desta licitação;

6.2.2.2. Aplicar à detentora da Ata as penalidades, quando for o caso;

6.2.2.3. Prestar à detentora da Ata toda e qualquer informação, por esta solicitada, necessária à perfeita execução do objeto;

6.2.2.4. Efetuar o pagamento à detentora da Ata no prazo, após a entrega da nota fiscal, devidamente atestada pelo fiscal e/ ou funcionário responsável;

6.2.2.5. Notificar, por escrito, à detentora da Ata da aplicação de qualquer sanção.

7 – CONTROLE E FISCALIZAÇÃO DO CONTRATO

7.1. A garantia deverá ser on-site, integral, para todos os Serviços, devendo ser prestada através da rede autorizada do fabricante. O tempo de garantia mínimo será de 12 (doze) meses. Dentro do prazo de validade do Contrato vigente.

7.2. Os serviços de suporte técnico serão solicitados mediante a abertura de chamados a serem efetuados por técnicos da Câmara de Vereadores, via chamada telefônica local ou 0800, e-mail, web site ou chat do fabricante ou à empresa autorizada, em qualquer caso em português, em horário comercial, feriados e fins de semana.

7.3. Todas as solicitações feitas pelo CONTRATANTE deverão ser registradas pela CONTRATADA para acompanhamento e controle da execução dos serviços.

7.4. O tempo de solução do chamado deve-se de forma **Imediata**.

7.5 O atendimento será do tipo "on-site" nas dependências da Câmara Municipal de Sinop, em dias úteis (segunda-feira à sexta-feira), no horário de expediente, por profissionais especializados e deverá cobrir todo e qualquer defeito apresentado, incluindo o fornecimento e a substituição de peças e/ou componentes, ajustes, reparos e correções necessárias para o correto funcionamento do Software.

8 – FORMA DE PAGAMENTO

8.1 A empresa CONTRATADA, após a prestação do serviço, deverá entregar a Câmara Municipal a NOTA FISCAL, para conferência e aprovação do objeto.

8.2 Após comprovada as exigências do objeto descrito com as exigências da habilitação, a Nota Fiscal será atestada pelo servidor responsável pela Administração da Câmara Municipal e entregue na contabilidade para efetivar o pagamento que será em até 30(trinta) dias. Apresentar juntamente a Nfe, o Certificado de Regularidade do FGTS, a Certidão Negativa de débitos relativos aos tributos Federais (PGFN) e a Certidão Negativa de Débitos Trabalhistas, Fazenda Estadual e Certidão Municipal.

8.3 A liberação da NFe para pagamento ficará condicionada ao atesto da unidade responsável pelo acompanhamento e recebimento do objeto contratado.

8.4 Quaisquer atraso ocorrido por parte da empresa vencedora na apresentação da fatura ou nota fiscal, ou dos documentos exigidos como condição para pagamento, imporá em prorrogação automática do prazo de vencimento da obrigação da Câmara Municipal.

8.5 Nenhum pagamento será efetuado enquanto pendente de liquidação, obrigação financeira imposta à CONTRATADA, em virtude de penalidade ou inadimplência, sem que o atraso gere direito a acréscimos de qualquer natureza.

8.6 As Notas Fiscais não poderão ter rasuras e deverão descrever corretamente o item, e número de empenho, o número do processo de compras, acompanhadas de boleto ou dados bancários para depósito.

8.7 Conforme a Instrução Normativa da Receita Federal do Brasil nº 1234/2012, suas

alterações ou outra norma que venha a substituí-la, regulamentada pelo Decreto Municipal nº 190/2023 para fins de retenção de Imposto de Renda, é condição para o recebimento e aceitação das notas fiscais e demais documentos de fornecimentos de materiais ou serviços, que o documento tenha destacado o valor do IRRF e que este seja deduzido em fatura ou eventual boleto para pagamento.

8.8 NÃO serão feitas retenções de CSLL, PIS/PASEP ou COFINS, apenas a retenção de IR, se for o caso, seja da administração direta, indireta ou fundações.

8.9 O pagamento será realizado através de boleto ou de ordem bancária, para crédito em banco, agência e conta-corrente, indicados pelo Contratado.

9 – FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

9.1 A licitação deverá ser realizada pelo critério do menor preço por item pela forma eletrônica para atingir um maior número de fornecedores e assim instigar a competitividade.

10 – CUSTO ESTIMADO DA CONTRATAÇÃO/PREÇO DE REFERÊNCIA

(mesma constante da Pesquisa de Preços)

11 – DOTAÇÃO ORÇAMENTÁRIA

01.031.0001.2005 Serviços de Tecnologia da Informação

3.3.90.40.00 Serviços de Tecnologia da Informação e Comunicação – Pessoa Jurídica

12 – DEMAIS INFORMAÇÕES ESPECÍFICAS DO PROJETO BÁSICO

12.1 O contrato oriundo desse será rescindida de pleno direito e para todos os fins em caso de liquidação ou dissolução, deferimento de concordata ou decretação de falência da detentora da mesma, independentemente de aviso, notificação ou interpelação judicial ou extrajudicial.

13 – GARANTIA DA CONTRATAÇÃO

13.1 Em conformidade com o disposto no art. 96 da Lei nº 14.133/2021, poderá ser exigida da contratada, como condição para assinatura do contrato, a prestação de garantia contratual com o objetivo de assegurar a fiel execução do objeto. A garantia poderá ser prestada em uma das seguintes modalidades:

13.1.1 Caução em dinheiro ou em títulos da dívida pública;

13.1.2 Seguro-garantia;

13.1.3 Fiança bancária;

13.1.4 O valor da garantia, quando exigido, será de até 5% (cinco por cento) do valor total do contrato, podendo ser elevado até 10% (dez por cento) nos casos de contratações de grande

vulto ou com alta complexidade técnica e riscos consideráveis

13.2. Garantia de segurança**:**

13.2.1 O provedor de nuvem deve garantir a segurança da cloud, incluindo a proteção da infra-estrutura, acesso, aplicação de patches, configuração de hosts, armazenamento e escalabilidade;

13.2.2 O provedor deve oferecer a estrutura adequada para a realização das políticas de backup;

13.3. Garantia de recuperação:

13.3.1 O backup em nuvem deve permitir recuperar os arquivos da empresa em caso de desastre, ataque ou sabotagem;

13.3.2 O backup em nuvem deve ser monitorado constantemente para garantir a segurança e o controle dos arquivos;

13.4. Segurança do armazenamento em nuvem:

13.4.1 A segurança do armazenamento em nuvem depende de vários fatores, incluindo o provedor de serviços escolhido e as práticas de segurança implementadas pelo usuário;

13.4.2 Para aumentar a segurança na nuvem, é possível usar autenticação multifatorial, monitorar e registrar as atividades dos usuários, realizarem um teste de intrusão e definir restrições de acesso;

13.5. Garantia Técnica dos Serviços Prestados**:**

13.5.1 A contratada deverá assegurar suporte técnico contínuo, manutenção corretiva e preventiva do sistema de firewall**,** incluindo:

13.5.2 Atendimento remoto ou presencial conforme criticidade;

13.5.3 Prazos de resposta e solução conforme níveis de serviço (SLA) definidos no contrato;

13.5.4 Substituição ou correção de falhas identificadas sem ônus adicional à Administração;

13.5.5 Atualização de firmware, assinaturas de segurança e licenciamento.

13.6. Responsabilidade Técnica:

13.6.1 Será exigida a apresentação de responsável técnico devidamente habilitado, com registro em conselho competente (ex: CREA ou CRA, conforme o caso).

13.7. Rastreabilidade e Logs de Auditoria**:**

13.7.1 Os sistemas de firewall deverão manter registros completos (logs) de acesso, alterações de configuração e tentativas de intrusão, com relatórios periódicos entregues à Administração.

13.8. Condições de Reversibilidade**:**

13.8.1 Em caso de rescisão contratual, deverão ser garantidas as condições de transferência do conhecimento técnico, configurações aplicadas e documentação completa do ambiente, de modo a permitir continuidade do serviço com outro fornecedor.

13.8.2 Esses requisitos visam assegurar não apenas a fiel execução contratual**,** mas também a qualidade, disponibilidade e segurança da rede institucional da Câmara Municipal de Sinop**,** sendo fundamentais para a preservação da integridade dos dados legislativos e administrativos.

13.9. Além disso, a empresa contratada deverá oferecer garantia técnica mínima de 12 (doze) meses sobre os serviços prestados, compreendendo o correto funcionamento das soluções implantadas (backup, firewall e cibersegurança com captive portal), bem como o suporte corretivo durante esse período, sem ônus adicional para a Administração Pública. A garantia técnica deverá incluir prazos definidos para atendimento e resolução de chamados, com penalidades previstas em caso de descumprimento.

13.10. O descumprimento injustificado das obrigações assumidas poderá acarretar a execução da garantia contratual e a aplicação das sanções administrativas previstas na legislação vigente.

Sinop/MT, 30 de Maio de 2025.

gov.br Documento assinado digitalmente
MAURO LAGNI
Data: 06/06/2025 10:55:51-0300
Verifique em https://validar.iti.gov.br

Mauro Lagni
Responsável pelo TR/PB

14 – CIÊNCIA DA AUTORIDADE COMPETENTE

(X) Concordo com o Termo de Referência/Projeto Básico realizado e **AUTORIZO** a contratação nos termos da Lei 14.133/2021.

Sinop/MT, 30 de Maio de 2025.

REMIDIO KUNTZ:36274526153
Assinado de forma digital por REMIDIO KUNTZ:36274526153
Dados: 2025.06.06 10:06:31 -04'00'

REMÍDIO KUNTZ
Presidente