ESTUDO TÉCNICO PRELIMINAR – ETP

1. NECESSIDADE DA CONTRATAÇÃO

1.1. A presente contratação visa atender à crescente demanda por uma infraestrutura de rede mais robusta, segura e eficiente, capaz de suportar as operações críticas da instituição e proteger seus ativos de informação contra ameaças cibernéticas cada vez mais sofisticadas. A solução proposta abrange o fornecimento de licenças de software, renovações de suporte e equipamentos para uma solução completa de segurança de rede, incluindo switches de rede corporativa, controle de acesso à rede (NAC), gerenciamento centralizado e solução de logs, análise e relatórios. A ausência de uma solução integrada e atualizada de segurança de rede pode resultar em vulnerabilidades significativas, comprometimento de dados, interrupção de serviços essenciais e não conformidade com regulamentações de segurança da informação. A modernização e aprimoramento da infraestrutura de segurança são cruciais para garantir a continuidade dos negócios, a proteção da privacidade dos dados e a integridade dos sistemas da instituição.

2. DEMONSTRAÇÃO DA PREVISÃO DA CONTRATAÇÃO NO PLANO DE CONTRATAÇÕES ANUAL

2.1. O Plano de Contratações para o Exercício 2024 não foi elaborado.

3. REQUISITOS DA CONTRATAÇÃO

3.1. A solução a ser contratada deve atender a um conjunto abrangente de requisitos, que visam garantir não apenas a conformidade técnica e funcional, mas também a aderência às normativas legais, às necessidades do negócio, aos padrões de segurança e privacidade, e às condições contratuais. Os requisitos estão sumarizados nas seguintes categorias:

3.1.1. Requisitos Legais

3.1.1.1. A CONTRATADA deverá assegurar que a solução e os serviços fornecidos estejam em plena conformidade com a legislação brasileira vigente, em especial:

I) Lei nº 14.133/2021 (Nova Lei de Licitações e Contratos Administrativos): Todos os aspectos da contratação, desde a fase de planejamento até a execução e fiscalização, deverão observar os princípios e as diretrizes estabelecidas por esta lei.

II) Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD): A solução deverá garantir a proteção dos dados pessoais tratados, em conformidade com os princípios da LGPD, incluindo a segurança, a privacidade, a transparência e o consentimento. A CONTRATADA deverá demonstrar a aderência da solução aos requisitos de segurança da informação da LGPD, especialmente no que tange ao tratamento de dados pessoais que possam transitar ou ser armazenados pelos sistemas de segurança de rede.

III) Marco Civil da Internet (Lei nº 12.965/2014): A solução deverá respeitar os princípios, garantias, direitos e deveres para o uso da Internet no Brasil, especialmente no que se refere à privacidade e à proteção dos dados pessoais.

3.1.2. Requisitos do Negócio

3.1.2.1. A solução deverá suportar e otimizar as operações de negócio da Câmara Municipal de Itanhaém, contribuindo para a eficiência, a produtividade e a continuidade dos serviços. Os requisitos de negócio incluem:

I) Disponibilidade e Continuidade: A solução deve garantir alta disponibilidade da infraestrutura de rede e dos serviços de segurança, minimizando interrupções e assegurando a continuidade das operações críticas da CONTRATANTE.

II) Desempenho: A solução deve proporcionar desempenho adequado para suportar o volume de tráfego da rede, sem comprometer a velocidade e a qualidade das comunicações.

III) Escalabilidade: A arquitetura da solução deve ser escalável, permitindo a expansão futura da capacidade para atender ao crescimento da demanda e à evolução das necessidades da CONTRATANTE.

IV) Gerenciamento Simplificado: A solução deve oferecer ferramentas de gerenciamento intuitivas e centralizadas, que facilitem a administração, o

monitoramento e a manutenção da infraestrutura de segurança, otimizando o tempo da equipe de TI.

V) Integração: A solução deve se integrar de forma transparente com a infraestrutura de rede e os sistemas de segurança existentes da CONTRATANTE, especialmente os equipamentos Fortinet, para garantir uma gestão coesa e eficiente.

VI) Rastreabilidade e Auditoria: A solução deve permitir a rastreabilidade de eventos e ações na rede, com registros detalhados para fins de auditoria e conformidade.

3.1.3. Requisitos de Segurança e Privacidade

3.1.3.1. A segurança e a privacidade são pilares fundamentais desta contratação. A solução deverá incorporar as melhores práticas e tecnologias para proteger os ativos de informação da CONTRATANTE. Os requisitos incluem:

I) Proteção Abrangente: A solução deve oferecer proteção multicamadas contra uma ampla gama de ameaças cibernéticas, incluindo malware, ransomware, ataques de negação de serviço (DDoS), intrusões, vazamento de dados e acessos não autorizados.

II) Controle de Acesso Robusto: Implementação de mecanismos de controle de acesso baseados em identidade, dispositivo e contexto, garantindo que apenas usuários e dispositivos autorizados acessem os recursos da rede.

III) Segmentação de Rede: Capacidade de segmentar a rede para isolar áreas críticas e limitar a propagação de ameaças em caso de comprometimento.

IV) Monitoramento e Detecção de Ameaças: Ferramentas de monitoramento em tempo real, detecção de anomalias e alertas proativos para identificar e responder rapidamente a incidentes de segurança.

V) Conformidade de Endpoint: Capacidade de verificar a conformidade de segurança dos dispositivos que se conectam à rede, garantindo que atendam aos padrões mínimos de segurança antes de conceder acesso.

VI) Privacidade dos Dados: A solução deve ser projetada para proteger a privacidade dos dados dos usuários, com funcionalidades que garantam a minimização da coleta, o tratamento adequado e a segurança das informações pessoais.

VII) Auditoria de Segurança: Geração de logs de segurança detalhados e imutáveis para fins de auditoria, investigação de incidentes e comprovação de conformidade.

3.1.4. Da Subcontratação

3.1.4.1. A contratada executará diretamente o objeto, sem transferência de responsabilidades ou subcontratações não autorizadas pela CONTRATANTE.

3.1.5. Da Garantia da Contratação

3.1.5.1. Não haverá exigência da garantia da contratação

4. ESTIMATIVAS DAS QUANTIDADES PARA A CONTRATAÇÃO

4.1. As quantidades estimadas para a contratação são as seguintes:

LOTE ÚNICO - SOLUÇÃO COMPLETA E INTEGRADA DE SEGURANÇA DE REDE			
ITEM	**DESCRIÇÃO**	**UNIDADE DE MEDIDA**	**QUANTIDADE**
1	Solução de Gerência Centralizada c/ Suporte p/ 03 (três) Anos	UNIDADE	1
2	Solução de Controle de Acesso à Rede c/ Suporte p/ 03 (três) Anos	UNIDADE	1
3	Licença para Controle de Acesso p/ 100 Devices c/ Suporte p/ 03 (três) Anos	UNIDADE	2
4	Solução de Gestão e Análise de Logs c/ Suporte p/ 03 (três) Anos	UNIDADE	1
5	Renovação de Licenças p/ Equipamentos Fortinet c/ Suporte p/ 03 (três) Anos	UNIDADE	2
6	Switch 48 Portas Gigabit Ethernet Full PoE c/ Suporte p/ 03 (três) Anos	UNIDADE	3

7	Switch 48 Portas Gigabit Ethernet c/ Suporte p/ 03 (três) Anos	UNIDADE	4
8	Serviços de Instalação e Configuração	UNIDADE	1

4.2. Com base no levantamento de mercado realizado, que considerou as fontes de pesquisa de preços, a identificação de potenciais fornecedores e a análise das soluções disponíveis, conclui-se que a solução da Fortinet é a mais adequada e vantajosa para a CONTRATANTE. Esta conclusão é fundamentada nos seguintes pontos: Compatibilidade e Integração:

4.2.1. A CONTRATANTE já possui uma infraestrutura de segurança de rede baseada em equipamentos Fortinet. A escolha de uma solução do mesmo fabricante garante a compatibilidade plena, a integração nativa entre os componentes (switches, NAC, gerenciamento centralizado, logs e firewalls existentes) e a otimização da gestão. A utilização de múltiplos fabricantes para componentes de segurança de rede pode gerar complexidade na integração, lacunas de segurança e dificuldades na manutenção e suporte.

4.2.2. Plataforma Unificada de Segurança: A Fortinet oferece uma plataforma de segurança unificada (Security Fabric) que permite uma visibilidade abrangente, controle centralizado e automação de políticas de segurança em toda a rede. Isso simplifica a administração, reduz a superfície de ataque e melhora a capacidade de detecção e resposta a ameaças.

4.2.3. Redução de Custos Operacionais: A padronização em um único fabricante para a solução de segurança de rede resulta em menores custos operacionais a longo prazo, devido à simplificação do treinamento da equipe, à otimização dos processos de suporte e manutenção, e à redução da complexidade na gestão de licenças e atualizações.

4.2.4. Experiência e Suporte: A Fortinet é líder de mercado em soluções de segurança de rede, com vasta experiência e uma rede global de suporte técnico. A

escolha de um fabricante consolidado garante a disponibilidade de suporte especializado e a continuidade das atualizações de segurança.

4.2.5. Desempenho Comprovado: As soluções Fortinet são reconhecidas pelo seu alto desempenho, escalabilidade e robustez, atendendo aos requisitos técnicos e funcionais exigidos pela CONTRATANTE para a proteção de sua infraestrutura de rede.

4.3. Diante do exposto, a contratação de uma solução completa de segurança de rede da Fortinet é a opção que melhor atende às necessidades da CONTRATANTE, proporcionando um ambiente de rede seguro, eficiente e gerenciável, com o melhor custo-benefício e alinhamento estratégico com a infraestrutura existente.

5. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

5.1. A estimativa do valor da contratação será realizada com base nos resultados do levantamento de mercado a ser conduzido, conforme o Art. 23 da Lei nº 14.133/2021.

5.2. Serão consideradas as propostas de fornecedores, preços praticados em contratações similares e dados de sistemas de compras governamentais, visando obter um valor de referência justo e compatível com o mercado para a solução completa de segurança de rede, incluindo licenças, renovações de suporte e equipamentos, bem como os serviços de instalação, implantação e treinamento.

6. DESCRIÇÃO DA SOLUÇÃO

6.1. A solução a ser contratada é um ecossistema de segurança de rede abrangente e integrado, projetado para fornecer proteção multicamadas, gerenciamento centralizado e visibilidade completa sobre o tráfego e os eventos da rede. A solução é composta pelos seguintes itens:

6.1.1. Solução de Gerência Centralizada c/ Suporte p/ 03 (três) Anos

6.1.1.1. Deve ser do tipo appliance virtual (VM);

6.1.1.2. Deverá possuir licenças de Garantia e Atualizações de Firmware pelo período de 36 (trinta e seis) meses;

6.1.1.3. Deve estar licenciado para gerenciar, no mínimo, 10 dispositivos;

6.1.1.4. Deverá ser compatível com os seguintes ambientes:

I) VMware ESXi 5.5, 6.0, 6.5, 6.7 e 7.0;

II) Microsoft Hyper-V 2008 R2/2012/2012 R2/2016;

III)Citrix XenServer 6.0+ e Open Source Xen 4.1+;

IV) KVM;

V) Nutanix AHV;

VI) Amazon Web Services (AWS);

VII) Microsoft Azure;

VIII) Google Cloud Platform (GCP);

IX) Oracle Cloud Infrastructure (OCI);

X) Alibaba Cloud (AliCloud);

6.1.1.5. Não deve possuir limite na quantidade de múltiplas vCPU;

6.1.1.6. Não deve possuir limite para suporte a expansão de memória RAM;

6.1.1.7. Deve suportar alta disponibilidade;

6.1.1.8. A plataforma deverá ser compatível com os atuais equipamentos de Firewall já utilizados na Câmara de Itanhaém, modelos FortiGate-100F de forma nativa e totalmente integrada;

6.1.1.9. Funcionalidades Gerais:

I) Deve ter a capacidade de permitir o provisionamento e o monitoramento da configuração SD-WAN de todos os dispositivos gerenciados a partir de um único console.

II) Como parte da visibilidade SD-WAN dos dispositivos gerenciados centralmente, a solução deve ter visibilidade do status do link, desempenho do aplicativo, utilização da largura de banda e conformidade com o SLA objetivo;

III)Deve ter a capacidade de automatizar fluxos de trabalho e configurações para dispositivos gerenciados em um único console;

IV) A solução deve ter o recurso de Multi-tenancy para separar os dados de gerenciamento da infraestrutura lógica ou geograficamente e permitir a implantação do zerotouch para o rápido provisionamento em massa;

V) A solução deve poder executar backups de configuração automáticos em até 5 nós, contendo atualizações de todos os dispositivos gerenciados;

VI) Deve ter a capacidade de permitir o provisionamento de comunidades VPN e monitorar as conexões VPN de todos os dispositivos gerenciados a partir de um único console e exibir sua localização geográfica em um mapa;

VII) A solução deve permitir o uso de APIs RESTful para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança;

VIII) Permite a integração de trocas e compartilhamento de dados com terceiros por meio do pxGrid, OCI, Esxi;

IX) Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

X) O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

XI) Permitir acesso concorrente de administradores

XII) Possuir interface baseada em linha de comando para administração da solução de gerência;

XIII) Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

XIV) Bloqueio de alterações, no caso de acesso simultâneo de dois ou mais administradores;

XV) Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

XVI) Gerar alertas automáticos via Email;

XVII) Gerar alertas automáticos via SNMP;

XVIII) Gerar alertas automáticos via Syslog;

XIX) Deve suportar backup/restore de todas as configurações da solução de gerência, permitindo ao administrador agendar backups da configuração em um determinado dia e hora;

XX) Deve ser permitido ao administrador transferir os backups para um servidor FTP;

XXI) Deve ser permitido ao administrador transferir os backups para um servidor SCP;

XXII) Deve ser permitido ao administrador transferir os backups para um servidor SFTP

XXIII) As alterações realizadas em um servidor de gerência deverão ser automaticamente replicadas para o servidor redundante;

XXIV) Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de contas de usuários LOCAIS;

XXV) Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de base externa TACACS;

XXVI) Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de usuários de base externa LDAP;

XXVII) Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de base externa RADIUS;

XXVIII) Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de Certificado Digital X.509 (PKI);

XXIX) Deve suportar sincronização do relógio interno via protocolo NTP;

XXX) Deve registrar as ações efetuadas por quaisquer usuários;

XXXI) Devem ser fornecidos manuais de instalação, configuração e operação de toda a solução, na língua portuguesa ou inglesa, com apresentação de boa qualidade;

XXXII) Suportar SNMP versão 2 e versão 3 nos equipamentos de gerência;

XXXIII) Deve permitir habilitar e desabilitar, para cada interface de rede da solução de gerência, permissões de acesso HTTP, HTTPS, SSH, SNMP e Telnet;

XXXIV) Deve permitir virtualizar a solução de gerência, de forma que cada administrador possa gerenciar, visualizar e editar apenas os dispositivos autorizados e cadastrados no seu ambiente virtualizado;

XXXV) A solução de gerência deve permitir criar administradores que tenham acesso à todas as instâncias de virtualização;

6.1.1.10. Funcionalidades de Gestão de Firewalls:

I) O gerenciamento deve possibilitar a criação e administração de políticas de firewall e controle de aplicação;

II) O gerenciamento deve possibilitar a criação e administração de políticas de IPS, Antivírus e Anti-Spyware;

III)O gerenciamento deve possibilitar a criação e administração de políticas de Filtro de URL;

IV) Permitir localizar quais regras um objeto está sendo utilizado;

V) Permitir criação de regras que fiquem ativas em horário definido;

VI) A solução deve permitir o repositório de assinaturas de antivírus, IPS, filtragem da Web e filtragem de email para otimizar a velocidade e o download centralizado de dispositivos gerenciados;

VII) Deve ter a capacidade de exibir os resultados da auditoria de segurança dos dispositivos gerenciados;

VIII) Permitir backup das configurações e rollback de configuração para a última configuração salva;

IX) Deve possuir mecanismo de Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

X) Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;

XI) Deve permitir que todos os firewalls sejam controlados de forma centralizada utilizando apenas um servidor de gerência;

XII) A solução deve incluir uma ferramenta para gerenciar centralmente as licenças de todos os appliances controlados pela estação de gerenciamento, permitindo ao administrador atualizar licenças nos appliances através dessa ferramenta;

XIII) A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos appliances;

XIV) Deve ser capaz de gerar relatórios ou exibir comparativos entre duas sessões diferentes, resumindo todas as alterações efetuadas;

XV) Deve permitir criar fluxos de aprovação na solução de gerência, onde um administrador possa criar todas as regras, mas as mesmas somente sejam aplicadas após aprovação de outro administrador;

XVI) Possuir "wizard" na solução de gerência para adicionar os dispositivos via interface gráfica utilizando IP, login e senha dos mesmos;

XVII) Permitir que eventuais políticas e objetos já presentes nos dispositivos sejam importados quando o mesmo for adicionado à solução de gerência;

XVIII) Permitir visualizar, a partir da estação de gerência centralizada, informações detalhadas dos dispositivos gerenciados, tais como hostname, serial, IP de gerência, licenças, horário do sistema e firmware;

XIX) Possuir "wizard" na solução de gerência para instalação de políticas e configurações dos dispositivos;

XX) Permitir criar na solução de gerência templates de configuração dos dispositivos com informações de DNS, SNMP, Configurações de LOG e Administração;

XXI) Permitir criar scripts personalizados, que sejam executados de forma centralizada em um ou mais dispositivos gerenciados com comandos de CLI dos mesmos;

XXII) Possuir histórico dos scripts executados nos dispositivos gerenciados pela solução de gerência;

XXIII) Permitir configurar e visualizar balanceamento de links nos dispositivos gerenciados de forma centralizada;

XXIV) Permitir criar vários pacotes de políticas que serão aplicados/associados à dispositivos ou grupos de dispositivos;

XXV) Deve permitir criar regras de NAT64 e NAT46 de forma centralizada;

XXVI) Permitir criar regras anti DoS de forma centralizada

XXVII) Permitir criar os objetos que serão utilizados nas políticas de forma centralizada;

XXVIII) Permitir criar, a partir da solução de gerência, VPNs entre os dispositivos gerenciados de forma centralizada, incluindo topologia (hub, spoke, dial-up), autenticações, chaves e métodos de criptografia;

XXIX) Deve permitir o uso de DDNS em VPNs de forma centralizada

XXX) Deve permitir o gerenciamento de pontos de acesso proprietários de forma centralizada;

XXXI) Deve permitir o gerenciamento centralizado dos switches a serem fornecidos neste processo de forma nativa e totalmente integrada

XXXII) Deve permitir o gerenciamento centralizado de perfis de segurança de software de forma nativa e totalmente integrada a atual plataforma de Firewall Modelo FortiGate-100F;

6.1.2. Solução de Controle de Acesso à Rede c/ Suporte p/ 03 (três) Anos

6.1.2.1. Solução de controle de acesso à redes, em formato de máquina virtual, a ser instalado em ambiente virtualizado disponibilizado pela CONTRATANTE;

6.1.2.2. Deverá possuir licenças de Garantia e Atualizações de Firmware pelo período de 36 (trinta e seis) meses;

6.1.2.3. Deve ser uma solução multi-vendor, suportando inclusive os switches e concentrador VPN do órgão;

6.1.2.4. A solução deve ser capaz de interoperar com dispositivos com e sem fios, dos principais fabricantes, incluindo, no mínimo:

I) Cisco/Meraki;

II) HP/HP Procurve/3Com/H3C;

III)Brocade/Motorola/Avaya/Extreme Networks/Enterasys;

IV) Fortinet/Meru;

V) Zimbro;

VI) Dell;

VII) Alcatel-Lucent;

VIII) ID-Link;

IX) Aruba;

X) Ruckus;

XI) Xirrus;

6.1.2.5. A solução deve permitir a integração de dispositivos de terceiros, incluindo:

I) NitroGuard IPS;

II) Sourcefire;

III)Meraki;

IV) Firewalls de Palo Alto;

V) Firewalls da Fortinet;

VI) Fire Eye;

VII) AirWatch;

VIII) MobileIron;

IX) MaaS360;

X) Citrix XenMobile;

XI) ADTRAN/BlueSocket;

6.1.2.6. A arquitetura da solução deve ser escalável, permitindo a ampliação de capacidade pela adição de novos appliances virtuais ou físicos, possibilitando que o licenciamento e o gerenciamento possam ser centralizados;

6.1.2.7. A solução deve suportar capacidade de expansão para até 25.000 endpoints simultâneos;

6.1.2.8. A solução deve ser capaz de inspecionar tanto IOT quanto estações/notebooks, sem depender de recursos como 802.1X e Mac-address bypass (MAB);

6.1.2.9. A utilização de 802.1x deve ser opcional, para controle de acesso de nível de porta da infra-estrutura cabeada;

6.1.2.10. Deve permitir a entrada de credenciais usando 802.1x ou Portal Captivo;

6.1.2.11. Para estações de trabalho, deve suportar compliance em VPN, seja IPsec ou SSL. Verificar SO, endpoints instalados, registros, serviços, arquivos etc;

6.1.2.12. A licença contemplada deverá suportar todas as características exigidas neste termo de referência;

6.1.2.13. A solução deve permitir diferentes perfis de administração, com a capacidade de limitar e controlar a quantidade de acesso permitido às funcionalidades disponíveis, dependendo do grupo administrativo da organização à qual o usuário pertence;

6.1.2.14. Deve detectar e classificar automaticamente o tipo dos dispositivos conectados na rede sem a necessidade de softwares instalados nos dispositivos;

6.1.2.15. Deve permitir determinar o perfil dos dispositivos descobertos por meio de métodos que não exigem a instalação de agentes, incluindo pelo menos os seguintes:

I) DHCP Fingerprint;

II) Consultas via protocolo HTTP/HTTPS;

III)Localização (dispositivo de acesso e porta);

IV) Consultas via protocolo SNMP;

V) Consultas via protocolo SSH;

VI) Consultas via protocolo Telnet;

VII) Consultas de portas TCP;

VIII) Consultas de portas UDP;

IX) MAC OUI;

X) Consultas via protocolo WMI;

XI) Protocolo ONVIF;

XII) WinRM;

XIII) Base assinaturas pré-definidas;

6.1.2.16. A solução deve ser capaz de reconhecer as seguintes informações sobre os dispositivos conectados à rede:

I) Endereço MAC;

II) Endereço IP;

III) Sistema operacional;

IV) Nome do host;

V) Horário de conexão;

VI) Usuário conectado;

VII) Localização;

6.1.2.17. A solução deve ser capaz de reconhecer, sem a necessidade de agentes instalados, os seguintes sistemas operacionais em execução nos dispositivos conectados à rede:

I) Android;

II) Apple iOS para iPhone, iPod e iPad;

III) BlackBerry OS/Blackberry OS 10;

IV) Chrome OS;

V) BSD gratuito;

VI) Kindle/Kindle Fire;

VII) Linux;

VIII) MacOS X;

IX) Open BSD;

X) Solaris;

XI) Symbian;

XII) Web OS;

XIII) Windows;

XIV) Windows Phone / CE/RT;

6.1.2.18. Deve lembrar o perfil atribuído a cada dispositivo e verificar se ainda é válido em cada conexão do dispositivo. Se o perfil variar, deve encerrar a conexão e notificar o evento;

6.1.2.19. Deve permitir a designação de um sponsor para autorizar a categorização dos dispositivos;

6.1.2.20. Deve permitir a categorização manual ou automática de dispositivos;

6.1.2.21. Deve permitir a recategorização periódica de dispositivos;

6.1.2.22. Permitir a importação de um arquivo CSV contendo informações sobre os dispositivos a serem registrados;

6.1.2.23. A solução deve incluir a detecção de dispositivos desconhecidos conectados à rede e adotar medidas de controle para limitar o acesso;

6.1.2.24. A solução deve suportar autenticação através de EAP-PEAP e EAP-TLS;

6.1.2.25. A solução deve suportar RADIUS Change of Authorization;

6.1.2.26. A solução deve suportar MAC Address Bypass;

6.1.2.27. A solução deve consultar bases LDAP e Active Directory para a identificação de usuários e grupos de usuários;

6.1.2.28. A solução deverá permitir a criação e aplicação de políticas de controle que combinem informações sobre a identidade do usuário e o tipo de dispositivo, possibilitando a autorização dinâmica de acesso à rede e a concessão de permissões com base em funções e diferentes níveis de acesso;

6.1.2.29. Deve habilitar a geração de políticas de controle, agrupadas hierarquicamente e determinar a diretiva para aplicar um conjunto de regras de mapeamento de cada dispositivo;

6.1.2.30. Deve permitir a definição dos horários em que os dispositivos serão autorizados a conectar na rede e avaliá-los periodicamente;

6.1.2.31. Deve suportar pelo menos os seguintes tipos de informações para determinar a diretiva a ser aplicada:

I) Localização;

II) Associação de grupo;

III)Atributo;

IV) Data e hora;

6.1.2.32. A solução deve ter capacidades BYOD/Onboarding;

6.1.2.33. Deve garantir a segmentação dinâmica da rede e aplicação de políticas de segurança, tendo como base variadas combinações, como login do AD e atributos (departamento, cidade, email, telefone), características da máquina (asset tag, hostname), localidade (switch, porta de switch, SSID) e horário;

6.1.2.34. A solução deve incluir recursos de gerenciamento de visitantes, permitindo a criação de diferentes perfis de utilização e autorização a serem associados aos usuários, distinguindo por exemplo prestadores de serviços dos visitantes;

6.1.2.35. A solução deve permitir o cadastro dos usuários visitantes na base interna da ferramenta para que não seja necessário realizar consultas em bases externas;

6.1.2.36. A solução deve possuir ferramenta que permita a geração automática de credenciais para usuários visitantes com login e respectivas senhas;

6.1.2.37. A solução deve possuir ferramenta que permita a criação de credenciais para eventos;

6.1.2.38. Deve permitir a definição de complexidade da senha dos usuários visitantes;

6.1.2.39. Deve ser possível definir um período de validade para as contas de usuários visitantes;

6.1.2.40. Deve ser possível definir data e horário para início e encerramento das contas de usuários visitantes;

6.1.2.41. A autenticação e autorização dos usuários visitantes deve ocorrer através de portal captivo acessível via browser web;

6.1.2.42. Os visitantes em hipótese alguma deverão ter acesso à Internet e rede interna antes que a autenticação seja concluída e o usuário seja autorizado;

6.1.2.43. Deve permitir a identificação de dispositivos usando o Portal Captivo, criação de perfil e classificação automáticas, autorização através de Radius, Active Directory e OpenLDAP e integração com plataformas MDM;

6.1.2.44. A solução deve vincular o login do visitante à máquina utilizada no acesso;

6.1.2.45. Deve suportar a validação de credenciais:

I) Em um banco de dados local;

II) Em servidores RADIUS;

III)Em servidores LDAP;

6.1.2.46. A solução deve ter a capacidade de utilizar a combinação de informações sobre a identidade do usuário e o tipo de dispositivo para acessar dinamicamente as permissões com base em funções e diferentes níveis de acesso;

6.1.2.47. A ferramenta deve permitir que os usuários visitantes possam realizar auto-registro através do preenchimento de cadastro disponível em portal web;

6.1.2.48. Deve permitir a customização dos campos obrigatórios e opcionais para o cadastro de auto-registro;

6.1.2.49. A solução deve permitir o envio da senha de acesso aos visitantes através de SMS e e-mail;

6.1.2.50. Deve ser possível definir um período para que os usuários visitantes sejam obrigados a se reautenticar;

6.1.2.51. A solução deve incluir recursos de IoT Onboarding com autorização dos sponsors;

6.1.2.52. A solução deve incluir a detecção e contenção de recursos de dispositivos desconhecidos (rogues);

6.1.2.53. A solução deve incluir recursos de conformidade de endpoint. Antes de permitir que dispositivos acessem a rede, deve checar que estes cumpram requisitos de segurança, integridade e configuração;

6.1.2.54. Deve permitir o uso de agentes persistentes, evanescentes (desaparecem após análise) e passivos;

6.1.2.55. Se um dispositivo não passar os testes de conformidade, deve ser possível:

I) Não forçar a remediação;

II) Forçar a remediação imediatamente, enviando o dispositivo à uma rede de quarentena;

III)Permita a remediação retardada, dando um período de tempo desde a detecção inicial à solução destes. Após o período de tolerância, caso os problemas persistam, o dispositivo deve ser colocado em quarentena imediatamente;

6.1.2.56. Deve permitir a designação de grupos de usuários com função de sponsor que ficarão responsáveis por autorizar o acesso dos usuários visitantes e prestadores de serviços;

6.1.2.57. Os usuários do tipo sponsor poderão cadastrar previamente um usuário visitante. O portal de cadastro e gerenciamento de usuários visitantes não deve permitir gerência administrativa dos demais recursos da solução;

6.1.2.58. A solução deve permitir a customização da aparência do captive portal, permitindo editar textos e inserir imagens;

6.1.2.59. Os usuários do tipo sponsor podem ser cadastrados na base local da ferramenta ou fazer parte de grupo de usuários em base LDAP/Active Directory;

6.1.2.60. A solução deve incluir recursos de conformidade de endpoint. Antes de permitir que os dispositivos acessem a rede, a solução deve garantir que estes cumpram requisitos de segurança, integridade e conformidade;

6.1.2.61. Deve permitir o uso de software agente instalado no dispositivo e agentes evanescentes que desaparecem após análise e não precisam ser instalados;

6.1.2.62. Tanto para IOTs quanto estações, se configurado, não devem ter qualquer acesso à redes de produção enquanto não forem inspecionados;

6.1.2.63. Se um dispositivo não passar os testes de conformidade, deve ser possível:

I) Não forçar a remediação;

II) Forçar a remediação imediatamente enviando o dispositivo à rede de quarentena;

III)Permitir a remediação retardada, ou seja, dando um período de tolerância para que o usuário corrija o problema. Caso os problemas persistam, o dispositivo deve ser colocado em quarentena;

6.1.2.64. A solução deve permitir verificações de conformidade em endpoints que façam uso do sistema operacional:

I) Windows 7;

II) Windows 8;

III)Windows 10;

IV) MacOS;

V) Linux;

VI) Android;

6.1.2.65. Para garantir a conformidade com as políticas de segurança, a solução deve permitir que sejam verificados os seguintes itens antes de autorizar o acesso de um endpoint na rede:

I) Presença de software de anti-vírus instalado e em execução;

II) Versão do sistema operacional;

III)Nome de domínio do Active Directory ao qual a estação Windows pertença;

IV) Serviços em execução para estações Windows;

V) Informações sobre um determinado certificado digital em estações Windows;

VI) Registros ou chaves de registro para estações Windows;

VII) Processos em execução para estações Windows, Linux e MacOS;

VIII) Arquivo armazenado em um determinado diretório para estações Windows, Linux e MacOS;

IX) Pacotes instalados em estações Linux e MacOS;

6.1.2.66. Suportar, através de upgrade de licenciamento, a integração com soluções de segurança da Fortinet, Palo Alto, FireEye, etc., para correlacionar alertas de segurança e restringir, isolar ou bloquear dispositivos comprometidos, reduzindo o tempo de contenção de ameaças;

6.1.2.67. Suportar, através de upgrade de licenciamento, um método genérico para integração de dispositivos, usando o recebimento, envio, análise e interpretação de mensagens Syslog;

6.1.2.68. A solução deve ser capaz de monitorar quando um serviço requerido for desabilitado ou interrompido em computadores. Além disso deve enviar a estação para quarentena de forma a garantir a conformidade com a política de segurança;

6.1.2.69. Deve possuir radius interno além de permitir o uso de radius externos;

6.1.2.70. Deve permitir a distribuição de agentes através, pelo menos, dos seguintes métodos:

I) Programas de gerenciamento e distribuição de software;

II) GPO do Active Directory;

III)Captive Portal;

6.1.2.71. Deve permitir a atualização automática ou programada dos agentes instalados nas máquinas;

6.1.2.72. O agente instalado nos computadores deve notificar os usuários com mensagens informativas em casos de eventos;

6.1.2.73. Quando em quarentena, um portal web deve ser apresentado aos usuários com informações sobre as razões pelas quais este foram movidos para o isolamento;

6.1.2.74. A solução deve compartilhar a identificação dos usuários e/ou dispositivos autenticados para a plataforma de segurança da rede via SSO, de forma que sejam vinculadas aos acessos de Internet, provendo rastreabilidade futura;

6.1.2.75. No que tange a compliance, quando houver sucesso, falha ou alerta, a solução deve permitir as seguintes ações: alerta, envio de e-mail e SMS, desabilitar o host, envio de mensagem direta para o host envolvido e rodar políticas adicionais de compliance;

6.1.2.76. A solução deve integrar com plataformas de MDM, suportando pelo menos: FortiClient, In Tune, Mobile Iron e Air Watch;

6.1.2.77. Deve suportar integração com soluções de patching;

6.1.2.78. Deve suportar integração com soluções de análise de vulnerabilidades;

6.1.2.79. A solução deve possuir dashboard que apresente informações e estatísticas relevantes de forma resumida;

6.1.2.80. A solução deve permitir a customização do dashboard para apresentar as informações que o administrador considera relevante;

6.1.2.81. A solução deverá disponibilizar relatórios predefinidos com informações abrangentes, incluindo, mas não se limitando a:

I) Registro de visitantes;

II) Registro de dispositivos;

III)Scan de dispositivos;

6.1.2.82. Deverá habilitar a geração e o arquivamento de relatórios periódicos;

6.1.2.83. Deverá permitir o envio automático de relatórios por e-mail;

6.1.2.84. Deve ter relatórios de conformidade PCI;

6.1.2.85. As informações nos relatórios devem ser capazes de ser exportadas no formato HTML, CSV, Excel, XML, RTF ou PDF;

6.1.2.86. Deve armazenar log de alarmes e permitir sua visualização e gerenciamento;

6.1.2.87. Alarmes de log devem ser capazes de ser ordenados por gravidade;

6.1.2.88. Permitir a eliminação de alarmes de log de forma manual ou automática;

6.1.2.89. Permitir a definição de alarmes em função da ocorrência de determinados eventos;

6.1.2.90. A solução deve permitir a consulta de informações e alteração de parâmetros de configuração via REST API;

6.1.2.91. A solução deve incluir um REST API que permite:

I) Informações detalhada de um elemento em particular, como um usuário ou um host;

II) Pesquisar o banco de dados para obter informações sobre um conjunto de dispositivos;

III)Atualizar os registros de usuários ou dispositivos;

IV) Bloquear ou desbloquear o acesso de um usuário a rede;

6.1.2.92. A solução deve armazenar os eventos internamente e permitir que sejam exportados;

6.1.2.93. A solução deve permitir a exportação dos eventos através de syslog;

6.1.2.94. Deve suportar alta disponibilidade, suportando todas os registros/autenticações caso um nó da solução esteja indisponível;

6.1.2.95. A solução deve suportar cenários onde as redes de serviço e produção são locais. Ou seja, sem necessidade de estender tais vlans até o NAC, que deverá ser capaz de gerenciá-las mesmo estando em subnets diversas;

6.1.2.96. A solução deve incluir uma faixa de auditoria de todas as ações e alterações feitas ao sistema pelos usuários administradores, incluindo o que foi alterado, quando foi alterado e quem o alterou;

6.1.2.97. Deve possibilitar o rastreio de dispositivos, notificando a localização dos mesmos quando se conectarem à rede;

6.1.2.98. Dentre os reports disponibilizados pela solução dedicada de logs, deve suportar reports de endpoints, por localidade, fabricante, inventário, devices registrados e rogues;

6.1.3. Licença para Controle de Acesso p/ 100 Devices c/ Suporte p/ 03 (três) Anos

6.1.3.1. A solução deve ser fornecida com pacotes de 100 endpoints conectados simultaneamente;

6.1.3.2. Os pacotes de licenças deverão possuir Garantia e Atualizações de Firmware pelo período de 36 (trinta e seis) meses;

6.1.4. Solução de Gestão e Análise de Logs c/ Suporte p/ 03 (três) Anos

6.1.4.1. Deve ser do mesmo fabricante da solução de firewall (NGFW) utilizada na Câmara de Itanhaém FortiGate-100F;

6.1.4.2. Deve ser do tipo appliance virtual (VM);

6.1.4.3. Deverá possuir licenças de Garantia e Atualizações de Firmware pelo período de 36 (trinta e seis) meses;

6.1.4.4. Possuir capacidade de recebimento de logs de pelo menos 10 mil dispositivos;

6.1.4.5. Possuir a capacidade de receber pelo menos 10 GBytes de logs diários;

6.1.4.6. Não deverá possuir limites de armazenamento de dados;

6.1.4.7. Deverá ser compatível com ambiente VMware ESXi 5.5, 6.0, 6.5, 6.7 e 7.0;

6.1.4.8. Deverá ser compatível com ambiente Microsoft Hyper-V 2008 R2/2012/2012 R2/2016/2019/2022;

6.1.4.9. Deverá ser compatível com ambiente Citrix XenServer 6.0+ e Open Source Xen 4.1+;

6.1.4.10. Deverá ser compatível com ambiente KVM;

6.1.4.11. Deverá ser compatível com ambiente Nutanix AHV;

6.1.4.12. Deverá ser compatível com ambiente Amazon Web Services (AWS);

6.1.4.13. Deverá ser compatível com ambiente Microsoft Azure;

6.1.4.14. Deverá ser compatível com o ambiente Google Cloud (GPC);

6.1.4.15. Deverá ser compatível com o ambiente Oracle Cloud Infrastructure (OCI);

6.1.4.16. Deverá ser compatível com o ambiente Alibaba Cloud (AliCloud);

6.1.4.17. Não deve possuir limite na quantidade de múltiplas vCPU;

6.1.4.18. Não deve possuir limite para suporte a expansão de memória RAM;

6.1.4.19. Deve suportar o acesso via SSH e WEB (HTTPS) para gerenciamento de soluções;

6.1.4.20. 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;

6.1.4.21. Permitir o acesso simultâneo à administração, bem como permitir que pelo menos 2 (dois) perfis sejam criados para administração e monitoramento;

6.1.4.22. Suportar SNMP versão 2 e 3;

6.1.4.23. Permitir a virtualização do gerenciamento e administração dos dispositivos, nos quais cada administrador só tem acesso aos computadores autorizados;

6.1.4.24. Permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução;

6.1.4.25. Permitir ativar e desativar para cada interface da plataforma, as permissões de acesso HTTP, HTTPS, SSH;

6.1.4.26. Possuir autenticação de usuários para acesso à plataforma via LDAP;

6.1.4.27. Possuir autenticação de usuários para acesso à plataforma via Radius;

6.1.4.28. Possuir autenticação de usuários para acesso à plataforma via TACACS +;

6.1.4.29. Possuir geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;

6.1.4.30. Possuir geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;

6.1.4.31. Possuir geração de relatórios de tráfego em tempo real, em formato de gráfico;

6.1.4.32. Possuir 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;

6.1.4.33. Possuir um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha;

6.1.4.34. Possuir visualização da quantidade de logs enviados de cada dispositivo monitorado;

6.1.4.35. Possuir mecanismos de apagamento automático para logs antigos;

6.1.4.36. Permitir importação e exportação de relatórios;

6.1.4.37. Deve ter a capacidade de criar relatórios no formato HTML;

6.1.4.38. Deve ter a capacidade de criar relatórios em formato PDF;

6.1.4.39. Deve ter a capacidade de criar relatórios no formato XML ;

6.1.4.40. Deve ter a capacidade de criar relatórios no formato CSV;

6.1.4.41. Deve permitir exportar os logs no formato CSV;

6.1.4.42. Deve gerar logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;

6.1.4.43. 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;

6.1.4.44. A solução deve ter relatórios predefinidos;

6.1.4.45. Deve poder enviar automaticamente os logs para um servidor FTP externo para a solução;

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

6.1.4.47. Ter a capacidade de personalizar a capa dos relatórios obtidos;

6.1.4.48. Permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos mesmos logs;

6.1.4.49. 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;

6.1.4.50. Ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;

6.1.4.51. Deve ter um mecanismo de "pesquisa detalhada" para navegar pelos relatórios em tempo real;

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

6.1.4.53. Ter a capacidade de gerar e enviar relatórios periódicos automaticamente;

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

6.1.4.55. Permitir o envio por e-mail relatórios automaticamente;

6.1.4.56. Deve permitir que o relatório seja enviado por e-mail ao destinatário específico;

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

6.1.4.58. É necessário exibir graficamente em tempo real a taxa de geração de logs para cada dispositivo gerenciado;

6.1.4.59. Deve permitir o uso de filtros nos relatórios;

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

6.1.4.61. Permitir especificar o idioma dos relatórios criados;

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

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

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

6.1.4.65. Possibilitar visualizar 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;

6.1.4.66. Deve ter uma ferramenta que permita analisar o desempenho na geração de relatórios, a fim de detectar e corrigir problemas na geração deles;

6.1.4.67. Importar arquivos com logs de dispositivos compatíveis conhecidos e não conhecidos pela plataforma, para geração posterior de relatórios;

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

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

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

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

6.1.4.72. Deve permitir visualizar em tempo real os logs recebidos;

6.1.4.73. Deve permitir o encaminhamento de log no formato syslog;

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

6.1.4.75. Deve incluir um painel para operações SOC que monitore as principais ameaças à segurança da sua rede;

6.1.4.76. Deve incluir o painel para operações do SOC que monitora o envolvimento do usuário e o uso suspeito da web em sua rede;

6.1.4.77. Deve incluir o painel para operações SOC que monitora o tráfego na sua rede;

6.1.4.78. Deve incluir o painel para operações SOC que monitoram o tráfego de aplicativos e sites na sua rede;

6.1.4.79. Deve incluir o painel para operações SOC que monitoram detecções de ameaças de dia zero em sua rede (sandboxing);

6.1.4.80. Deve incluir o painel para operações SOC que monitora a atividade do terminal na sua rede;

6.1.4.81. Deve incluir o painel para operações SOC que monitoram a atividade da VPN na sua rede;

6.1.4.82. Deve incluir um painel para operações SOC que monitora pontos de acesso Wi-Fi e SSIDs;

6.1.4.83. Deve incluir o painel para operações SOC que monitoram o desempenho dos recursos locais da solução (CPU, Memória);

6.1.4.84. Deve permitir a criação de painéis personalizados para monitorar operações SOC;

6.1.4.85. Suportar a configuração Master / Slave de alta disponibilidade na camada 3;

6.1.4.86. Gerar alertas de eventos a partir de logs recebidos;

6.1.4.87. Permitir a criação de incidentes a partir de alertas de eventos para o terminal;

6.1.4.88. Permitir a integração ao sistema de tickets do ServiceNow;

6.1.4.89. Oferecer suporte ao serviço Indicadores de Comprometimento (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, veredicto (classificação geral da ameaça), o número de ameaças detectadas;

6.1.4.90. Deve permitir o suporte a logs na nuvem pública do Amazon S3;

6.1.4.91. Deve permitir o suporte a logs na nuvem pública do Microsoft Azure;

6.1.4.92. Permitir o suporte aos registros de nuvem pública do Gooogle Cloud;

6.1.4.93. Suportar o padrão SAML para autenticação do usuário administrador;

6.1.4.94. Deve ter um relatório de conformidade com o PCI DSS;

6.1.4.95. Possuir um relatório de uso do aplicativo SaaS;

6.1.4.96. Possuir um relatório de prevenção de perda de dados (DLP);

6.1.4.97. Possuir um relatório de VPN;

6.1.4.98. Possuir um relatório IPS (Intruder Prevention System);

6.1.4.99. Possuir um relatório de reputação do cliente ;

6.1.4.100. Possuir um relatório de análise de segurança do usuário;

6.1.4.101. Possuir um relatório de análise de ameaças cibernéticas;

6.1.4.102. Possuir um breve relatório resumido diário de eventos e incidentes de segurança;

6.1.4.103. Possuir um relatório de tráfego DNS;

6.1.4.104. Possuir um relatório de tráfego de e-mail;

6.1.4.105. Possuir um relatório dos 10 principais aplicativos usados na rede;

6.1.4.106. Possuir um relatório dos 10 principais sites usados na rede;

6.1.4.107. Possuir um relatório de uso de mídia social;

6.1.5. Renovação de Licenças p/ Equipamentos Fortinet c/ Suporte p/ 03 (três) Anos

6.1.5.1. Renovação da Solução Fortigate 100F UTP Bundle:

I) SKU: FC-10-F100F-950-02-36;

II) Período: 36 (trinta e seis) meses;

III)Seriais contemplados:

a) FG100FTK23000180;

b) FG100FTK23004438;

IV) A renovação solicitada deve abranger, obrigatoriamente, os seguintes serviços:

a) Hardware - Advanced HW;

b) Firmware e Atualizações Gerais - Web/Online;

c) Suporte Avançado (Enhanced Support) – Premium;

d) Suporte Telefônico – Premium;

e) Proteção Avançada contra Malware (Advanced Malware Protection) - Web/Online;

f) Serviço IPS FortiGuard - Web/Online;

g) Serviço de Filtragem de URL, DNS e Vídeo FortiGuard - Web/Online;

h) AntiSpam - Web/Online;

V) Observação:

a) O período de vigência da renovação deverá ser contado a partir da data de vencimento da licença atual, ou seja, a partir de 20/03/2026;

6.1.6. Switch 48 Portas Gigabit Ethernet Full PoE c/ Suporte p/ 03 (três) Anos

6.1.6.1. A Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 2 do modelo OSI;

6.1.6.2. Deverá possuir licenças de Garantia e Atualizações de Firmware pelo período de 36 (trinta e seis) meses;

6.1.6.3. Deve possuir 48 (quarenta e oito) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);

6.1.6.4. Adicionalmente, deve possuir 04 (quatro) slots SFP+ para conexão de fibras ópticas operando em 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;

6.1.6.5. Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 720W;

6.1.6.6. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial;

6.1.6.7. Deve possuir capacidade de comutação de pelo menos 170 Gbps e ser capaz de encaminhar até 250 Mpps (milhões de pacotes por segundo);

6.1.6.8. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;

6.1.6.9. Deve possuir tabela MAC com suporte a 30.000 endereços;

6.1.6.10. Deve implementar Flow Control baseado no padrão IEEE 802.3X;

6.1.6.11. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);

6.1.6.12. Deve suportar a comutação de Jumbo Frames;

6.1.6.13. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;

6.1.6.14. Deve implementar serviço de DHCP Relay;

6.1.6.15. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 500 (quinhentos) entradas na tabela;

6.1.6.16. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring);

6.1.6.17. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree).

6.1.6.18. Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;

6.1.6.19. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;

6.1.6.20. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra ataques do tipo “Denial of Service” no ambiente nível 2;

6.1.6.21. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

6.1.6.22. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;

6.1.6.23. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;

6.1.6.24. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;

6.1.6.25. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, campo CoS e VLAN ID;

6.1.6.26. Deve suportar a definição de dias e horários que a ACL deverá ser aplicada na rede;

6.1.6.27. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);

6.1.6.28. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;

6.1.6.29. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;

6.1.6.30. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

6.1.6.31. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;

6.1.6.32. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;

6.1.6.33. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;

6.1.6.34. Deve suportar MAC Authentication Bypass (MAB);

6.1.6.35. Deve implementar RADIUS CoA (Change of Authorization);

6.1.6.36. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;

6.1.6.37. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;

6.1.6.38. Deve implementar Guest VLAN para aqueles usuários que não autenticam nas interfaces em que o IEEE 802.1X estiver habilitado;

6.1.6.39. Deve ser capaz de operar em modo de monitoramento para autenticação 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como re-configurar a interface;

6.1.6.40. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;

6.1.6.41. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;

6.1.6.42. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;

6.1.6.43. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);

6.1.6.44. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;

6.1.6.45. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;

6.1.6.46. Deve suportar o envio de mensagens de log para servidores externos através de syslog;

6.1.6.47. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;

6.1.6.48. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);

6.1.6.49. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;

6.1.6.50. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);

6.1.6.51. Deve permitir ser gerenciado através de IPv6;

6.1.6.52. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;

6.1.6.53. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;

6.1.6.54. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;

6.1.6.55. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;

6.1.6.56. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch;

6.1.6.57. Deverá suportar ser configurado e monitorado através de REST API;

6.1.6.58. Deve em conjunto com a controladora ser capaz de implementar e orquestrar políticas de segurança de micro segmentação nos switches controlando como os usuários/endpoints se comunicam lateralmente entre si;

6.1.6.59. Deve em conjunto com a controladora permitir a criação de automações que executem ações baseadas em eventos de rede detectados no ambiente, como quarentenar um dispositivo, isolar um endpoint, implementar e/ou ajustar políticas de segurança dependendo do evento detectado, de forma automatizada.

6.1.6.60. Deve suportar temperatura de operação de até 40° Celsius;

6.1.6.61. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;

6.1.6.62. Deve ser fornecido com fonte de alimentação com capacidade para operar em tensões de 110V e 220V;

6.1.6.63. Deve ser compatível e gerenciado pela atual solução existente marca FORTINET modelo FortiGate-100F ou por solução do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:

I) A solução de gerência centralizada deve suportar operação com elementos redundantes, não havendo disrupção do serviço mediante a falha de um elemento;

II) Deve operar como ponto central para automação e gerenciamento dos switches;

III)Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches;

IV) Deve possuir interface gráfica para configuração, administração e monitoração dos switches;

V) Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede;

VI) Deve montar a topologia da rede de maneira automática;

VII) Deve ser capaz de configurar os switches da rede;

VIII) Deve através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribui-las automaticamente em todos os switches gerenciados;

IX) Deve através da interface gráfica deve ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;

X) Deve através da interface gráfica ser capaz de aplicar as políticas de QoS nas interfaces dos switches;

XI) Deve através da interface gráfica ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;

XII) Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;

XIII) Deve através da interface gráfica ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard;

XIV) Deve através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;

XV) A solução de gerência centralizada deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection);

XVI) Deve ser capaz de configurar parâmetros SNMP dos switches;

XVII) A solução de gerência centralizada deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente;

XVIII) A solução de gerência centralizada deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas;

XIX) A solução de gerência centralizada deve apresentar graficamente informações sobre erros nas interfaces dos switches;

XX) A solução deve apresentar graficamente informações sobre disponibilidade dos switches;

XXI) Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;

XXII) Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede;

XXIII) Deve possuir API no formato REST;

6.1.7. Switch 48 Portas Gigabit Ethernet c/ Suporte p/ 03 (três) Anos

6.1.7.1. A Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 2 do modelo OSI;

6.1.7.2. Deverá possuir licenças de Garantia e Atualizações de Firmware pelo período de 36 (trinta e seis) meses;

6.1.7.3. Deve possuir 48 (quarenta e oito) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);

6.1.7.4. Adicionalmente, deve possuir 04 (quatro) slots SFP+ para conexão de fibras ópticas operando em 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;

6.1.7.5. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial;

6.1.7.6. Deve possuir capacidade de comutação de pelo menos 170 Gbps e ser capaz de encaminhar até 250 Mpps (milhões de pacotes por segundo);

6.1.7.7. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;

6.1.7.8. Deve possuir tabela MAC com suporte a 30.000 endereços;

6.1.7.9. Deve implementar Flow Control baseado no padrão IEEE 802.3X;

6.1.7.10. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);

6.1.7.11. Deve suportar a comutação de Jumbo Frames;

6.1.7.12. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;

6.1.7.13. Deve implementar serviço de DHCP Relay;

6.1.7.14. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 500 (quinhentos) entradas na tabela;

6.1.7.15. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring);

6.1.7.16. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree).

6.1.7.17. Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;

6.1.7.18. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;

6.1.7.19. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra ataques do tipo “Denial of Service” no ambiente nível 2;

6.1.7.20. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

6.1.7.21. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;

6.1.7.22. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;

6.1.7.23. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;

6.1.7.24. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, campo CoS e VLAN ID;

6.1.7.25. Deve suportar a definição de dias e horários que a ACL deverá ser aplicada na rede;

6.1.7.26. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);

6.1.7.27. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;

6.1.7.28. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;

6.1.7.29. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

6.1.7.30. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;

6.1.7.31. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;

6.1.7.32. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;

6.1.7.33. Deve suportar MAC Authentication Bypass (MAB);

6.1.7.34. Deve implementar RADIUS CoA (Change of Authorization);

6.1.7.35. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;

6.1.7.36. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;

6.1.7.37. Deve implementar Guest VLAN para aqueles usuários que não autenticam nas interfaces em que o IEEE 802.1X estiver habilitado;

6.1.7.38. Deve ser capaz de operar em modo de monitoramento para autenticação 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como re-configurar a interface;

6.1.7.39. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;

6.1.7.40. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;

6.1.7.41. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;

6.1.7.42. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);

6.1.7.43. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;

6.1.7.44. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;

6.1.7.45. Deve suportar o envio de mensagens de log para servidores externos através de syslog;

6.1.7.46. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;

6.1.7.47. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);

6.1.7.48. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;

6.1.7.49. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);

6.1.7.50. Deve permitir ser gerenciado através de IPv6;

6.1.7.51. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;

6.1.7.52. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;

6.1.7.53. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;

6.1.7.54. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;

6.1.7.55. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch;

6.1.7.56. Deverá suportar ser configurado e monitorado através de REST API;

6.1.7.57. Deve em conjunto com a controladora ser capaz de implementar e orquestrar políticas de segurança de micro segmentação nos switches controlando como os usuários/endpoints se comunicam lateralmente entre si.

6.1.7.58. Deve em conjunto com a controladora permitir a criação de automações que executem ações baseadas em eventos de rede detectados no ambiente, como quarentenar um dispositivo, isolar um endpoint, implementar e/ou ajustar políticas de segurança dependendo do evento detectado, de forma automatizada.

6.1.7.59. Deve suportar temperatura de operação de até 40º Celsius;

6.1.7.60. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;

6.1.7.61. Deve ser fornecido com fonte de alimentação com capacidade para operar em tensões de 110V e 220V;

6.1.7.62. Deve ser compatível e gerenciado pela atual solução existente marca FORTINET modelo FortiGate-100F ou por solução do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:

I) A solução de gerência centralizada deve suportar operação com elementos redundantes, não havendo disrupção do serviço mediante a falha de um elemento;

II) Deve operar como ponto central para automação e gerenciamento dos switches;

III)Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches;

IV) Deve possuir interface gráfica para configuração, administração e monitoração dos switches;

V) Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede;

VI) Deve montar a topologia da rede de maneira automática;

VII) Deve ser capaz de configurar os switches da rede;

VIII) Deve através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribui-las automaticamente em todos os switches gerenciados;

IX) Deve através da interface gráfica deve ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;

X) Deve através da interface gráfica ser capaz de aplicar as políticas de QoS nas interfaces dos switches;

XI) Deve através da interface gráfica ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;

XII) Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;

XIII) Deve através da interface gráfica ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard;

XIV) Deve através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;

XV) A solução de gerência centralizada deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection);

XVI) Deve ser capaz de configurar parâmetros SNMP dos switches;

XVII) A solução de gerência centralizada deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente;

XVIII) A solução de gerência centralizada deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas;

XIX) A solução de gerência centralizada deve apresentar graficamente informações sobre erros nas interfaces dos switches;

XX) A solução deve apresentar graficamente informações sobre disponibilidade dos switches;

XXI) Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;

XXII) Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede;

XXIII) Deve possuir API no formato REST;

6.1.8. Serviços de instalação e configuração

6.1.8.1. A realização dos serviços de instalação e configuração deverá ser realizado em até 30 dias do recebimento dos equipamentos e licenças pela CONTRATANTE. O serviço deverá ser realizado de forma on-site nas dependências da CONTRATANTE;

6.1.8.2. O planejamento dos serviços de instalação deve resultar num documento tipo SOW (em tradução livre, escopo de trabalho). Neste documento devem conter a relação, descrição e quantidades dos produtos fornecidos, descrição da infraestrutura existente e desejada, detalhamento dos serviços que serão executados, premissas do projeto, locais e horários de execução dos serviços, condições de execução dos serviços, pontos de contato da CONTRATADA e CONTRATANTE, cronograma de execução do projeto em etapas, com responsáveis e data de início e fim (se aplicável), relação da documentação a ser entregue ao final da execução dos serviços, responsabilidade da CONTRATADA, plano de gerenciamento de mudanças, itens excluídos no projeto e termo de aceite. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes;

6.1.8.3. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, devendo a CONTRATADA sugerir as configurações de acordo com normas técnicas e boas práticas, cabendo à CONTRATANTE a sua aceitação expressa ou recusa nos casos de não atendimento das condições estabelecidas;

6.1.8.4. Após a instalação, a solução deverá ser monitorada de forma remota pelo prazo mínimo de 8 (oito) horas corridas, observando as condições de funcionamento e performance dos equipamentos, sendo possível o troubleshooting em caso de problemas ou não conformidades na operação;

6.1.8.5. Ao final da instalação, deverá ser realizado o repasse de configurações hands-on, de forma remota, apresentando as configurações realizadas nos equipamentos pelo prazo mínimo de 8 (oito) horas corridas;

6.1.8.6. Os serviços deverão ser realizados por pessoal técnico experiente e certificado pelo fabricante dos equipamentos. A Contratante solicitará os comprovantes da qualificação profissional do(s) técnico(s) que executará(ão) os serviços, sendo direito da mesma a sua aceitação ou exigência de troca de profissional no caso de este não satisfazer às condições supramencionadas;

6.1.8.7. Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados no projeto (relatório as-built), etapas de execução e toda informação pertinente para posterior continuidade e manutenção da solução instalada, como usuários e endereços de acesso, configurações realizadas e o resumo das configurações dos equipamentos. Este relatório deve ser enviado com todas as informações em até 15 (quinze) dias após a finalização dos serviços;

6.1.8.8. CONTRATADA deverá garantir a confidencialidade das informações, dados e senhas compartilhadas da CONTRATANTE;

6.1.8.9. Durante as atividades realizadas na prestação do serviço, o técnico da CONTRATADA deverá demonstrar à equipe técnica de acompanhamento da CONTRATANTE como instalar e configurar os equipamentos e os softwares fornecidos (instalação assistida).

7. DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS EM TERMOS DE ECONOMICIDADE E DE MELHOR APROVEITAMENTO DOS RECURSOS HUMANOS, MATERIAIS OU FINANCEIROS DISPONÍVEIS

7.1. A contratação da solução completa de segurança de rede visa alcançar uma série de resultados positivos em termos de economicidade e otimização de recursos, conforme detalhado a seguir:

7.1.1. A principal meta é fortalecer a postura de segurança da instituição, protegendo dados sensíveis, sistemas críticos e a privacidade dos usuários contra uma gama crescente de ameaças cibernéticas. Isso reduzirá significativamente o risco de incidentes de segurança, como vazamento de dados, ataques de ransomware e interrupções de serviço, que podem gerar custos financeiros elevados (multas, recuperação de dados, perda de reputação) e danos irreparáveis à imagem da instituição.

7.1.2. A solução integrada e centralizada permitirá que a equipe de TI gerencie a segurança da rede de forma mais eficiente. A automação de tarefas, a visibilidade aprimorada e a simplificação das operações reduzirão a carga de trabalho manual,

liberando a equipe para focar em atividades mais estratégicas e de maior valor agregado. Isso se traduz em melhor aproveitamento do capital humano, sem a necessidade de expandir o quadro de pessoal para lidar com a complexidade crescente da segurança de rede.

7.1.3. A solução proposta, ao consolidar diversas funcionalidades de segurança em uma plataforma unificada, evita a necessidade de adquirir e manter múltiplos equipamentos e softwares de diferentes fornecedores. Isso otimiza o uso do espaço físico, reduz o consumo de energia e simplifica a manutenção do hardware. A compatibilidade com a infraestrutura Fortinet existente maximiza o investimento prévio em equipamentos, garantindo que os novos componentes se integrem perfeitamente ao ambiente atual.

7.1.4. Embora represente um investimento inicial, a solução completa de segurança de rede proporcionará economicidade a longo prazo. A prevenção de incidentes de segurança, a redução do tempo de inatividade, a otimização da gestão e a consolidação de tecnologias resultarão em menores custos operacionais e de manutenção. Além disso, a renovação de licenças e suporte por 36 meses garante a continuidade do serviço e o acesso a atualizações críticas, protegendo o investimento e evitando gastos emergenciais com a substituição de tecnologias obsoletas ou vulneráveis.

7.1.5. A solução auxiliará a instituição a cumprir com as exigências da Lei Geral de Proteção de Dados (LGPD) e outras regulamentações de segurança da informação, evitando sanções legais e financeiras decorrentes da não conformidade.

7.1.6. Com switches de alta performance e um controle de acesso robusto, a solução contribuirá para uma rede mais estável, rápida e disponível, impactando positivamente a produtividade dos usuários e a qualidade dos serviços prestados pela instituição. Em suma, a contratação desta solução não é apenas uma medida de segurança, mas um investimento estratégico que trará retornos significativos em termos de eficiência operacional, redução de riscos e otimização do uso dos recursos disponíveis.

8. PROVIDÊNCIAS A SEREM ADOTADAS PELA ADMINISTRAÇÃO PREVIAMENTE À CELEBRAÇÃO DO CONTRATO

8.1. Não há providências a serem adotadas.

9. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

9.1. Não há correlação com outras contratações.

10. DESCRIÇÃO DE POSSÍVEIS IMPACTOS AMBIENTAIS E RESPECTIVAS MEDIDAS MITIGADORAS

10.1. Nesta contratação não existem possíveis impactos ambientais e respectivas medidas de tratamento.

11. POSICIONAMENTO CONCLUSIVO SOBRE A ADEQUAÇÃO DA CONTRATAÇÃO PARA O ATENDIMENTO DA NECESSIDADE A QUE SE DESTINA

11.1. A contratação requerida alinha-se às finalidades da Câmara Municipal e mostra-se viável sob as óticas ambiental, econômico e estratégica, conforme demonstrado neste estudo;

11.2. Os requisitos relevantes para a contratação foram devidamente levantados e analisados;

11.3. As quantidades são condizentes com a demanda prevista;

11.4. Existe no mercado a solução proposta que garante a concorrência;

11.5. A estimativa preliminar de preços foi realizada e documentada;

11.6. Foram indicados os resultados pretendidos com a contratação.

Itanhaém, data da assinatura eletrônica.

ALLAN BELLUCCI
DIRETOR DE TECNOLOGIA DA INFORMAÇÃO