

TERMO DE REFERÊNCIA

COMPANHIA DE SANEAMENTO DE SERGIPE – DESO
PREGÃO ELETRÔNICO Nº /2023-DGC
Processo Administrativo nº /2023

1 – OBJETO

O presente processo consiste na realização de Pregão Eletrônico para Registro de Preços para aquisição de Equipamentos de Segurança e Gerência de Redes, englobando o fornecimento de todo hardware, software, subscrições, serviços de implantação e suporte técnico, visando futuras contratações, de acordo com a conveniência e a necessidade do CONTRATANTE conforme especificações constantes neste Termo de Referência.

2 – JUSTIFICATIVA

2.1 – DO OBJETO

A Tecnologia da Informação é um dos principais agentes de mudanças organizacionais. Sua utilização deve atentar-se para as questões estratégicas de apoio à integração operacional, organizacional e funcional. A correta utilização dos recursos da tecnologia contribui para um ambiente institucional moderno, integrando as ações de todos os setores, fazendo da informatização um fator crítico de sucesso institucional.

Com o dinamismo no surgimento de novas tecnologias e a crescente demanda, à necessidade permanente em manter-se alta disponibilidade, alto desempenho, segurança e controle para que todos os usuários, das redes dependentes direta ou indiretamente da DESO, possam exercer suas atividades de rotina proporcionando melhor qualidade nas ações corporativas.

Diante do exposto, e com o avanço cada vez mais expressivo das técnicas de exploração de vulnerabilidade, entende-se a necessidade de ampliação das camadas de proteção de cyber segurança neste ambiente, visando a ampliação da maturidade das soluções de rede e segurança que permitam evitar possíveis ataques a rede de dados da DESO.

2.2. DA METODOLOGIA DO PREÇO MÁXIMO

A metodologia utilizada para definição do preço máximo de referência foi o preço médio da pesquisa de mercado.

2.3. DO QUANTITATIVO

Levando em consideração que teremos equipamentos vencendo garantia em 2023 e uma grande parte em 2024, registraremos os preços para o quantitativo de todo o parque de Firewall's da rede da DESO por 1 (um) ano.

O objeto foi agrupado em lote único em razão da integração e compatibilidade entre os itens do presente Termo com nossa solução de segurança implantada, é recomendado que os produtos sejam compatíveis para evitarmos prejuízos futuros para esta Companhia.

3 – QUANTIDADE E DESCRIÇÃO DOS SERVIÇOS

3.1 – LOTE ÚNICO

ITEM	DESCRIPTIVO	Unidade	Quantidade
1	Solução de Segurança E Gerência de Rede NGFW – Tipo I	unid	120
2	Solução de Segurança E Gerência de Rede NGFW – Tipo II	unid	04
3	Solução de Ativos de Rede – SWITCH	unid	30
4	Solução de Ativo de Rede Wireless	unid	30
5	Solução para Duplo Fator de Autenticação - Token TIPO I (pacote com 10 unidades)	unid	15
6	Solução para Duplo Fator de Autenticação - Token TIPO II (pacote com 10 unidades)	unid	5

4 – ESTIMATIVA DO VALOR DO OBJETO DA CONTRATAÇÃO

Na orçamentação do objeto foram realizadas consultas no mercado para compor os preços e buscar atender ao previsto no RILC da Companhia de Saneamento de Sergipe – DESO a partir de pesquisa junto a prestadores de serviços.

5 – DA QUALIFICAÇÃO TÉCNICA

5.1 – A LICITANTE deve apresentar o atestado de capacidade técnica emitido por empresa pública ou privada comprovando que prestou serviços de instalação e configuração e todo suporte técnico devido durante a vigência contratual para os equipamentos do item 1 e 2 do Item 3.1 deste Termo de Referência com características semelhantes às especificadas neste Termo de Referência. Para tanto, exige-se um ou mais atestados cujo somatório seja no mínimo 50% do quantitativo total estimado para os itens de maior relevância, neste caso, os itens 1 e 2 do Item 3.1 deste Termo de Referência. Este percentual se justifica em razão da necessidade de comprovação da capacidade técnico operacional da licitante. Para tanto a licitante deve observar as especificações abaixo:

5.1.1 – Os atestados deverão ser impressos em papel timbrado, com nome e telefone de contato dos responsáveis pela informação atestada, não sendo aceitas declarações genéricas, devendo ainda atestar a satisfação com o serviço ofertado pela LICITANTE.

5.1.2 – A CONTRATANTE se reserva o direito de conferir as informações prestadas pelas empresas emitentes dos atestados, através de consultas e visitas, bem como a disponibilidade de equipamentos solicitados junto à LICITANTE.

5.1.3 – A LICITANTE deve apresentar declaração de que dispõe de mão-de-obra adequada e disponível, além de local para execução dos serviços técnicos. Deverão ser apresentados, no mínimo, 02 (dois) profissionais técnicos, integrantes do quadro da empresa sócio e/ou funcionário e/ou prestadores de serviços devidamente treinados pelo fabricante para instalar, configurar e manter os itens ofertados, devendo estes treinamentos técnicos serem comprovados por certificados de qualificação técnica vigentes.

6 – ESPECIFICAÇÕES TÉCNICAS

6.1 – ITEM 01 – SOLUÇÃO DE SEGURANÇA E GERÊNCIA DE REDE NGFW – TIPO I

6.1.1 – CARACTERÍSTICAS DO EQUIPAMENTO:

6.1.1.1 – Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.

6.1.1.2 – A solução poderá ser composta por mais de um equipamento para atender as funcionalidades exigidas, desde que todos os itens sejam do mesmo fabricante garantindo total compatibilidade e integração, desde que ocupem até 4U, no máximo.

6.1.1.3 – Deve possuir e estar licenciado durante a vigência contratual de 48 (quarenta e oito meses),

minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPsec e SSL, Controle de Aplicações, DLP – Data Leak Prevention e contextos virtuais

6.1.1.4 – Deve possuir fonte de alimentação com chaveamento automático 110/220V.

6.1.1.5 – Deve possuir Firewall com capacidade mínima de processamento de 5 (cinco) Gbps.

6.1.1.6 – Deve possuir IPS com capacidade mínima de processamento de 1 (um) Gbps.

6.1.1.7 – Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 500 (quinhentos) Mbps, contemplando as funções de Firewall, IPS, controle de aplicação e proteção contra Malware/Antivírus ativadas de maneira simultâneas.

6.1.1.8 – Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 300 (trezentos) Mbps.

6.1.1.9 – Deve possuir VPN com capacidade de, pelo menos, 4 (quatro) Gbps de tráfego IPsec.

6.1.1.10 – Deve suportar 600.000 (seiscentos mil) conexões simultâneas.

6.1.1.11 – Deverão ser licenciados para suportar, pelo menos, 150 (cento e cinquenta) usuários de VPN SSL.

6.1.1.12 – Deve suportar, pelo menos, 30.000 (trinta mil) novas conexões por segundo.

6.1.1.13 – Deve suportar, pelo menos, 150 (cento e cinquenta) túneis de VPN Site-Site.

6.1.1.14 – Deve suportar, pelo menos, 200 (duzentos) túneis de VPN Client-Site.

6.1.1.15 – Deve possuir, pelo menos, 5 (cinco) interfaces RJ 45.

6.1.1.16 – Deve ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 6 (seis) equipamentos.

6.1.1.17 – Deve ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 6 (seis) equipamentos.

6.1.1.18 – Deve ser fornecida Solução de Gerência Centralizada de Equipamentos, caso compatível poderá ser utilizada atual solução existente na DESO, Marca Fortinet, Modelo FMG-VM.

6.1.1.19 – Deve ser fornecida Solução Centralizada de Armazenamento de Logs e Relatórios, caso compatível poderá ser utilizada atual solução existente na DESO, Marca Fortinet, Modelo FAZ-VM.

6.1.1.20 – Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.

6.1.1.21 – Deve ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês.

6.2 – ITEM 02 – SOLUÇÃO DE SEGURANÇA E GERÊNCIA DE REDE NGFW – TIPO II

6.2.1 – CARACTERÍSTICAS DO EQUIPAMENTO:

6.2.1.1 – Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.

6.2.1.2 – A solução poderá ser composta por mais de um equipamento para atender as funcionalidades exigidas, desde que todos os itens sejam do mesmo fabricante garantindo total compatibilidade e integração, desde que ocupem até 4U, no máximo.

6.2.1.3 – Deve possuir e estar licenciado durante a vigência contratual de 48 (quarenta e oito meses), minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, DLP – Data Leak Prevention e contextos virtuais

6.2.1.4 – Deve possuir fonte de alimentação com chaveamento automático 110/220V redundante. A fonte fornecida Deve suportar sozinha a operação da unidade com todos os módulos de interface ativos.

6.2.1.5 – Deve possuir firewall com capacidade mínima de processamento de 11 (onze) Gbps.

6.2.1.6 – Deve possuir IPS com capacidade mínima de processamento de 4 (quatro) Gbps.

6.2.1.7 – Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 3 (três) Gbps, contemplando as funções de Firewall, IPS, controle de aplicação e proteção contra Malware/Antivírus ativadas de maneira simultâneas.

6.2.1.8 – Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 3 (três) Gbps.

6.2.1.9 – Deve possuir VPN com capacidade de, pelo menos, 10 (dez) Gbps de tráfego IPSec.

6.2.1.10 – Deve suportar 2.500.000 (dois milhões e quinhentas mil) conexões simultâneas.

6.2.1.11 – Deverão ser licenciados para suportar, pelo menos, 400 (quatrocentos) usuários de VPN SSL.

6.2.1.12 – Deve suportar, pelo menos, 200.000 (duzentos mil) novas conexões por segundo.

6.2.1.13 – Deve suportar, pelo menos, 1.500 (mil e quinhentos) túneis de VPN Site-Site.

6.2.1.14 – Deve suportar, pelo menos, 10.000 (dez mil) túneis de VPN Client-Site.

6.2.1.15 – Deve possuir, pelo menos, 04 (quatro) interfaces SFP+ 10GE.

6.2.1.16 – Deve possuir, pelo menos, 06 (seis) interfaces SFP 1GE.

6.2.1.17 – Deve possuir, pelo menos, 14 (quatorze) interfaces RJ 45.

6.2.1.18 – Deve incluir licença para a funcionalidade de VPN SSL.

6.2.1.19 – Deve ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 100

(cem) equipamentos.

6.2.1.20 – Deve ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 60 (sessenta) equipamentos.

6.2.1.21 – Deve ser fornecida Solução de Gerência Centralizada de Equipamentos, caso compatível poderá ser utilizada atual solução existente na DESO, Marca Fortinet, Modelo FMG-VM.

6.2.1.22 – Deve ser fornecida Solução Centralizada de Armazenamento de Logs e Relatórios, caso compatível poderá ser utilizada atual solução existente na DESO, Marca Fortinet, Modelo FAZ-VM.

6.2.1.23 – Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.

6.2.1.24 – Deve ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês.

6.3 – REQUISITOS GERAIS DE FUNCIONALIDADES E LICENCIAMENTOS COMUNS A TODOS OS MODELOS ACIMA (SOLUÇÕES DE SEGURANÇA E GERÊNCIA DE REDE - NGFW TIPO “I”, “II”)

6.3.1 – FUNCIONALIDADES ESPECÍFICAS

6.3.1.1 – Deve possuir controle de acesso à internet por endereço IP de origem e destino;

6.3.1.2 – Deve possuir controle de acesso à internet por sub rede;

6.3.1.3 – Deve suportar tags de VLAN (802.1q);

6.3.1.4 – Deve possuir ferramenta de diagnóstico do tipo tcpdump;

6.3.1.5 – Deve possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;

6.3.1.6 – Deve possuir integração com tokens para autenticação de 02 (dois) fatores;

6.3.1.7 – Deve suportar single-sign-on para Active Directory, RADIUS;

6.3.1.8 – Deve possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);

6.3.1.9 – Deve possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, vários para um, NAT64, NAT46, PAT, STUN e Full Cone NAT;

6.3.1.10 – Deve permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de

políticas por horários e por dia da semana;

6.3.1.11 – Deve permitir controle de acesso à internet por domínio, por exemplo: gov.br, org.br, edu.br;

6.3.1.12 – Deve possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT;

6.3.1.13 – Deve suportar roteamento estático e dinâmico RIP V1, V2, OSPF, ISIS e BGPv4;

6.3.1.14 – Deve possuir funcionalidades de DHCP Cliente, Servidor e Relay;

6.3.1.15 – Deve suportar aplicações multimídia, como: H.323 e SIP;

6.3.1.16 – Deve possuir tecnologia de firewall do tipo Statefull;

6.3.1.17 – Deve suportar alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;

6.3.1.18 – Deve permitir o funcionamento em modo transparente tipo “bridge” sem alterar o endereço MAC do tráfego;

6.3.1.19 – Deve suportar PBR – Policy Based Routing;

6.3.1.20 – Deve permitir a criação de VLANS no padrão IEEE 802.1q;

6.3.1.21 – Deve possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto em CLI (linha de comando);

6.3.1.22 – Deve permitir filtro de pacotes sem controle de estado (stateless) para verificação em camada 2;

6.3.1.23 – Deve permitir forwarding de camada 2 para protocolos não IP;

6.3.1.24 – Deve suportar forwarding multicast;

6.3.1.25 – Deve suportar roteamento multicast PIM Sparse Mode e Dense Mode;

6.3.1.26 – Deve permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos: TCP, UDP, ICMP e IP;

6.3.1.27 – Deve permitir o agrupamento de serviços;

6.3.1.28 – Deve permitir o filtro de pacotes sem a utilização de NAT;

6.3.1.29 – Deve permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;

6.3.1.30 – Deve possuir mecanismo de anti-spoofing;

6.3.1.31 – Deve permitir criação de regras definidas pelo usuário;

6.3.1.32 – Deve permitir o serviço de autenticação para tráfego HTTP e FTP;

6.3.1.33 – Deve permitir IP/MAC binding, permitindo que cada endereço IP possa ser associado a um endereço MAC, gerando maior controle dos endereços internos e impedindo o IP spoofing;

6.3.1.34 – Deve possuir a funcionalidade de balanceamento e contingência de links;

6.3.1.35 – Deve suportar sFlow;

6.3.1.36 – O dispositivo deve ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas.

6.3.1.37 – Deve ter a capacidade de permitir a criação de regras de firewall específicas para tipos de dispositivos identificados automaticamente (funcionalidade está conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Linux e Windows;

6.3.1.38 – Deve ter a capacidade de criar e aplicar políticas de reputação de cliente para registrar e pontuar as seguintes atividades: tentativas de conexões más, pacotes bloqueados por política, detecção de ataques de intrusão, detecção de ataques de malware, atividades Web em categorias de risco, proteção de aplicação, locais geográficos que os clientes estão tentando se comunicar;

6.3.1.39 – Deve permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;

6.3.1.40 – Deve permitir a criação de regras baseada em usuário, grupo de usuários, endereço IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação;

6.3.1.41 – Deve suportar certificados X.509, SCEP, Certificate Signing Request (CSR) e OCSP;

6.3.1.42 – Deve permitir funcionamento em modo bridge, router, proxy explícito, sniffer e/ou VLAN-tagged;

6.3.1.43 – Deve possuir mecanismo de tratamento (session-helpers ou ALGs) para os protocolos ou aplicações dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 O, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS;

6.3.1.44 – Deve suportar SIP, H.323 e SCCP NAT Traversal;

6.3.1.45 – Deve permitir a criação de objetos e agrupamento de objetos de usuários, redes, FQDN, protocolos e serviços para facilitar a criação de regras;

6.3.1.46 – Deve possuir porta de comunicação serial ou USB para testes e configuração do equipamento, com acesso protegido por usuário e senha.

6.3.2 – FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

6.3.2.1 – Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;

6.3.2.2 – Deve permitir modificação de valores DSCP para o DiffServ;

6.3.2.3 – Deve permitir priorização de tráfego e suportar ToS;

6.3.2.4 – Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web;

6.3.2.5 – Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

6.3.2.6 – Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;

6.3.2.7 – Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;

6.3.2.8 – Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação;

6.3.2.9 – Deve controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino;

6.3.2.10 – Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;

6.3.2.11 – Deve ter a capacidade de permitir a criação de perfis de controle de banda específicos para tipos de dispositivos identificados automaticamente (funcionalidade esta conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Linux e Windows.

6.3.3 – FUNCIONALIDADE DE ANTI-SPAM DE GATEWAY

6.3.3.1 – Deve permitir, na funcionalidade de anti-spam, verificação do cabeçalho SMTP do tipo MIME;

6.3.3.2 – Deve possuir filtragem de e-mail por palavras chaves;

6.3.3.3 – Deve permitir adicionar rótulo ao assunto da mensagem quando classificado como SPAM;

6.3.3.4 – Deve possuir, para a funcionalidade de anti-spam, o recurso de RBL;

6.3.3.5 – Deve permitir a checagem de reputação da URL no corpo mensagem de correio eletrônico;

6.3.3.6 – Deve ter a capacidade de permitir a criação de perfis de anti-spam específicos para tipos de dispositivos identificados automaticamente (funcionalidade está conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Linux e Windows.

6.3.4 – FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

6.3.4.1 – Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança;

6.3.4.2 – Deve possuir, pelo menos, 70 (setenta) categorias para classificação de sites Web;

6.3.4.3 – Deve possuir base mínima contendo 100.000.000 (cem milhões) de sites internet Web já

registrados e classificados;

6.3.4.4 – Deve possuir a funcionalidade de cota de tempo de utilização por categoria;

6.3.4.5 – Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como:

6.3.4.5.1 – Proxy anônimo;

6.3.4.5.2 – Webmail;

6.3.4.5.3 – Instituições de saúde;

6.3.4.5.4 – Notícias;

6.3.4.5.5 – Phishing;

6.3.4.5.6 – Hackers;

6.3.4.5.7 – Pornografia;

6.3.4.5.8 – Racismo;

6.3.4.5.9 – Websites pessoais;

6.3.4.5.10 – Compras;

6.3.4.6 – Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;

6.3.4.7 – Deve permitir a criação de, pelo menos, 07 (sete) categorias personalizadas;

6.3.4.8 – Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP;

6.3.4.9 – Deve prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado toda vez que quando houver tentativa de acesso a determinado serviço permitido ou bloqueado;

6.3.4.10 – Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;

6.3.4.11 – Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

6.3.4.12 – Deve possuir integração com tokens para autenticação de 02 (dois) fatores;

6.3.4.13 – Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança;

6.3.4.14 – Deve permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies e activeX, através de base de URL própria atualizável;

6.3.4.15 – Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual;

6.3.4.16 – Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e

bloqueadas (lista negra);

6.3.4.17 – Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido;

6.3.4.18 – Deve filtrar o conteúdo baseado em categorias em tempo real;

6.3.4.19 – Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web;

6.3.4.20 – Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;

6.3.4.21 – Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

6.3.4.22 – Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem;

6.3.4.23 – Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP;

6.3.4.24 – Deve permitir o bloqueio de redirecionamento HTTP;

6.3.4.25 – Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams;

6.3.4.26 – Deve possuir Proxy Explícito e Transparente;

6.3.4.27 – Deve implementar roteamento WCCP e ICAP;

6.3.4.28 – Deve ter a capacidade de permitir a criação de perfis de filtragem Web específicos para tipos de dispositivos identificados automaticamente (funcionalidade está conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Linux e Windows.

6.3.5 – FUNCIONALIDADE DE DETECÇÃO DE INTRUSÃO

6.3.5.1 – Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão;

6.3.5.2 – Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas;

6.3.5.3 – Deve estar orientado à proteção de redes;

6.3.5.4 – Deve permitir funcionar em modo transparente, sniffer e router;

6.3.5.5 – Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;

6.3.5.6 – Deve permitir a criação de padrões de ataque manualmente;

6.3.5.7 – Deve possuir integração à plataforma de segurança;

6.3.5.8 – Deve possuir capacidade de remontagem de pacotes para identificação de ataques;

- 6.3.5.9 – Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web;
- 6.3.5.10 – Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;
- 6.3.5.11 – Deve ter a capacidade de permitir a criação de perfis de inspeção específicos para tipos de dispositivos identificados automaticamente (funcionalidade está conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Linux e Windows;
- 6.3.5.12 – Deve possuir mecanismos de detecção/proteção de ataques;
- 6.3.5.13 – Deve possuir reconhecimento de padrões;
- 6.3.5.14 – Deve possuir análise de protocolos;
- 6.3.5.15 – Deve possuir detecção de anomalias;
- 6.3.5.16 – Deve possuir detecção de ataques de RPC (Remote Procedure Call);
- 6.3.5.17 – Deve possuir proteção contra-ataques de Windows ou NetBios;
- 6.3.5.18 – Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol);
- 6.3.5.19 – Deve possuir proteção contra-ataques DNS (Domain Name System);
- 6.3.5.20 – Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin;
- 6.3.5.21 – Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol);
- 6.3.5.22 – Deve possuir métodos de notificação de detecção de ataques;
- 6.3.5.23 – Deve possuir alarmes na console de administração;
- 6.3.5.24 – Deve possuir alertas via correio eletrônico;
- 6.3.5.25 – Deve possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo Deve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;
- 6.3.5.26 – Deve ter a capacidade de resposta/logs ativa a ataques;
- 6.3.5.27 – Deve prover a terminação de sessões via TCP resets;
- 6.3.5.28 – Deve armazenar os logs de sessões;
- 6.3.5.29 – Deve atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;
- 6.3.5.30 – Deve mitigar os efeitos dos ataques de negação de serviços;
- 6.3.5.31 – Deve permitir a criação de assinaturas personalizadas;

- 6.3.5.32 – Deve possuir filtros de ataques por anomalias;
- 6.3.5.33 – Deve permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;
- 6.3.5.34 – Deve permitir filtros de anomalias de protocolos;
- 6.3.5.35 – Deve suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;
- 6.3.5.36 – Deve suportar verificação de ataque na camada de aplicação;
- 6.3.5.37 – Deve suportar verificação de tráfego em tempo real, via aceleração de hardware;
- 6.3.5.38 – Deve possuir as seguintes estratégias de bloqueio: pass, drop e reset.

6.3.6 – FUNCIONALIDADE DE VPN

- 6.3.6.1 – Deve possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;
- 6.3.6.2 – Deve possuir suporte a certificados PKI X.509 para construção de VPNs;
- 6.3.6.3 – Deve possuir suporte a VPNs IPsec Site-to-Site e VPNs IPsec Client-to-Site;
- 6.3.6.4 – Deve possuir suporte a VPN SSL;
- 6.3.6.5 – Deve possuir capacidade de realizar SSL VPNs utilizando certificados digitais;
- 6.3.6.6 – A VPN SSL Deve possibilitar o acesso a toda infraestrutura, de acordo com a política de segurança, através de um plug-in ActiveX e/ou Java;
- 6.3.6.7 – Deve possuir hardware acelerador criptográfico para incrementar o desempenho da VPN;
- 6.3.6.8 – A VPN SSL Deve suportar cliente para plataforma Windows, Linux e Mac OS X;
- 6.3.6.9 – Deve permitir a arquitetura de VPN hub and spoke;
- 6.3.6.10 – Deve possuir suporte à inclusão em autoridades certificadoras (enrollment), mediante SCEP (Simple Certificate Enrollment Protocol) e mediante arquivos.

6.3.7 – FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

- 6.3.7.1 – Deve reconhecer, no mínimo, 2.000 (duas mil) aplicações;
- 6.3.7.2 – Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações;
- 6.3.7.3 – Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como:
 - 6.3.7.3.1 – P2P
 - 6.3.7.3.2 – Instant Messaging;
 - 6.3.7.3.3 – Web client;
 - 6.3.7.3.4 – Transferência de arquivos;
 - 6.3.7.3.5 – VoIP;
- 6.3.7.4 – Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;
- 6.3.7.5 – Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados,

identificando-as apenas pelo comportamento de tráfego da mesma;

6.3.7.6 – Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

6.3.7.7 – Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

6.3.7.8 – Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;

6.3.7.9 – Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;

6.3.7.10 – Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

6.3.7.11 – Deve possuir integração com tokens para autenticação de 02 (dois) fatores;

6.3.7.12 – Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;

6.3.7.13 – Deve permitir a inspeção/bloqueio de códigos maliciosos para, no mínimo, as seguintes categorias: Instant Messaging e transferência de arquivos;

6.3.7.14 – Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações;

6.3.7.15 – Deve permitir criação de padrões de aplicação manualmente;

6.3.7.16 – Deve ter a capacidade de permitir a criação de perfis de controle de aplicações específicos para tipos de dispositivos identificados automaticamente (funcionalidade está conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Linux e Windows.

6.3.8 – FUNCIONALIDADE DE DLP (DATA LEAK PREVENTION)

6.3.8.1 – O sistema de DLP (Data Leak Prevention – Proteção contra Vazamento de Informações) de gateway Deve funcionar de maneira que se consiga que os dados sensíveis não saiam da rede e também Deve funcionar de modo que se previna que dados não requisitados entrem na sua rede;

6.3.8.2 – Deve inspecionar, no mínimo, os tráfegos de e-mail, HTTP;

6.3.8.3 – Sobre o tráfego de e-mail, Deve inspecionar, no mínimo, os protocolos SMTP, POP3 e IMAP;

6.3.8.4 – Deve realizar buscas para a aplicação de regras de DLP em arquivos do tipo PDF e MS-Word;

6.3.8.5 – Deve fazer a varredura no conteúdo de um cookie HTTP buscando por determinado texto;

6.3.8.6 – Deve aplicar regras baseadas em usuários autenticados, isto é, fazendo buscas pelo tráfego de um específico usuário;

6.3.8.7 – Deve verificar para aplicações do tipo e-mail, se o anexo das mensagens de correio

entrantes/saintes possui um tamanho máximo especificado pelo administrador;

6.3.8.8 – Deve utilizar expressões regulares para composição das regras de verificação dos tráfegos;

6.3.8.9 – Deve tomar minimamente as ações de bloquear, banir usuário e colocar em quarentena a interface sobre as regras que coincidirem com o tráfego esperado pela regra;

6.3.8.10 – Deve permitir o armazenamento em solução específica de armazenamento de logs, o conteúdo do tráfego que coincidir com o tráfego esperado pela regra de DLP para minimamente os protocolos de e-mail, HTTP e mensageiros instantâneos;

6.3.8.11 – Deve permitir a composição de múltiplas regras de DLP, formando uma regra única mais específica que usa lógica booleana para fazer a comparação com o tráfego que atravessa o sistema.

6.3.9 – FUNCIONALIDADE DE BALANCEAMENTO DE CARGA

6.3.9.1 – Deve permitir a criação de endereços IPs virtuais;

6.3.9.2 – Deve permitir balanceamento de carga entre, pelo menos, 04 (quatro) servidores reais;

6.3.9.3 – Deve suportar balanceamento, ao menos, para os seguintes serviços: HTTP, HTTPS, TCP e UDP;

6.3.9.4 – Deve permitir balanceamento, ao menos, com os seguintes métodos: Hash do endereço IP de origem, Static, Round Robin, Weighted, First Alive e HTTP host, Least Session, Least RTT;

6.3.9.5 – Deve permitir persistência de sessão por cookie HTTP ou SSL session ID;

6.3.9.6 – Deve permitir que seja mantido o IP de origem;

6.3.9.7 – Deve suportar SSL offloading nos equipamentos que suportem, pelo menos, 200 (duzentos) usuários;

6.3.9.8 – Deve ter a capacidade de identificar, através de health checks, quais os servidores que estejam ativos, removendo automaticamente o tráfego dos servidores que não estejam;

6.3.9.9 – Deve permitir que o health check seja feito, ao menos, via ICMP, TCP em porta configurável e HTTP em URL configurável.

6.3.10 – FUNCIONALIDADE DE VIRTUALIZAÇÃO

6.3.10.1 – Deve suportar a criação de, ao menos, 10 (dez) instâncias virtuais no mesmo hardware;

6.3.10.2 – Deve permitir a criação de administradores independentes para cada uma das instâncias virtuais;

6.3.10.3 – Deve permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.

6.3.11 – FUNCIONALIDADE DE CONTROLADORA WIRELESS E WI-FI

6.3.11.1 – Deverá ser capaz de gerenciar, de forma centralizada, outros Pontos de Acesso do mesmo

fabricante;

6.3.11.2 – Deverá suportar o serviço de servidor DHCP por SSID para prover endereçamento IP automático para os clientes wireless;

6.3.11.3 – Deverá suportar monitoração e supressão de Ponto de Acesso indevido;

6.3.11.4 – Deverá prover autenticação para a rede wireless através de bases externas, como: LDAP, RADIUS ou TACACS+;

6.3.11.5 – Deverá permitir a visualização dos clientes conectados;

6.3.11.6 – Deverá prover suporte a Fast Roaming;

6.3.11.7 – Deverá ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF;

6.3.11.8 – A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;

6.3.11.9 – Deverá possuir Captive Portal por SSID;

6.3.11.10 – Deverá permitir configurar o bloqueio de tráfego entre SSIDs;

6.3.11.11 – Deverá suportar Wi-Fi Protected Access (WPA), WPA2 ou WPA3 por SSID, utilizando-se de AES e/ou TKIP;

6.3.11.12 – Deverá suportar os seguintes métodos de autenticação EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-SIM, EAP-AKA;

6.3.11.13 – Deverá suportar 802.1x através de RADIUS;

6.3.11.14 – Deverá suportar filtro baseado em endereço MAC por SSID;

6.3.11.15 – Deverá permitir configurar parâmetros de rádio, como: banda e canal;

6.3.11.16 – Deverá possuir método de descoberta de novos Pontos de Acesso baseados em Broadcast ou Multicast;

6.3.11.17 – Deverá possuir mecanismo de identificação e controle de rogue APs, suportando supressão automática e bloqueio por endereço MAC de APs;

6.3.11.18 – Deverá possuir lista contendo Pontos de Acesso Aceitos e Pontos de Acesso Indevidos (Rogue);

6.3.11.19 – Deverá possuir WIDS com, ao menos, os seguintes perfis:

6.3.11.19.1 – Rogue/Interfering AP Detection;

6.3.11.19.2 – Ad-hoc Network Detection;

- 6.3.11.19.3 – Wireless Bridge Detection;
- 6.3.11.19.4 – Weak WEP Detection;
- 6.3.11.19.5 – MAC OUI Checking;
- 6.3.11.20 – Deverá permitir o uso de voz e dados sobre um mesmo SSID;
- 6.3.11.21 – A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm;
- 6.3.11.22 – A controladora deverá oferecer Firewall integrado, baseado em identidade do usuário;
- 6.3.11.23 – Deverá possuir controle baseado em política de firewall para acesso entre as WLANs;
- 6.3.11.24 – Deverá permitir a criação de políticas de traffic shaping;
- 6.3.11.25 – Deverá permitir a criação de políticas de firewall baseadas em horário;
- 6.3.11.26 – Deverá permitir NAT nas políticas de firewall;
- 6.3.11.27 – Deverá possibilitar definir número de clientes por SSID;
- 6.3.11.28 – Deverá permitir e/ou bloquear o tráfego entre SSIDs;
- 6.3.11.29 – Deverá possuir mecanismo de criação automática de usuários visitantes e senhas autogeradas e/ou manual, que possam ser enviadas por e-mail ou SMS aos usuários, e com capacidade de definição de horário da expiração da senha;
- 6.3.11.30 – A comunicação entre o Access Point e a Controladora Wireless deverá poder ser efetuada de forma criptografada;
- 6.3.11.31 – Deverá possuir mecanismo de ajuste de potência do sinal, de forma a reduzir interferência entre canais entre 02 (dois) Access Points gerenciados;
- 6.3.11.32 – Deverá possuir mecanismo de balanceamento de tráfego/usuários entre Access Points;
- 6.3.11.33 – Deverá possuir mecanismo de balanceamento de tráfego/usuários entre frequências e/ou rádios;
- 6.3.11.34 – Toda a configuração do Ponto de Acesso deverá ser executada através da Controladora Wireless;
- 6.3.11.35 – Deverá permitir a identificação de APs com firmware desatualizado e efetuar o upgrade via interface gráfica;
- 6.3.11.36 – Deverá possuir console de monitoramento dos usuários conectados, indicando em que Access Point, em que rádio, em que canal, endereço IP do usuário, tipo de dispositivo e sistema operacional, uso de banda, potência do sinal e relação sinal/ruído;
- 6.3.11.37 – O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste

modo todos os pacotes trafegados em um determinado SSID devem ser encaminhados dentro do túnel até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional do próprio fabricante para suportar a conexão dos túneis originados dos pontos de acesso;

6.3.11.38 – A Controladora deverá oferecer Firewall integrado, baseado em identidade do usuário, entre todas as redes cujo tráfego seja tunelado até a Controladora;

6.3.11.39 – Deverá possuir controle baseado em política de firewall para acesso entre as WLANs cujo tráfego seja tunelado até a Controladora;

6.3.11.40 – Deverá permitir a criação de políticas de traffic shaping entre todas as redes cujo tráfego seja tunelado até a Controladora;

6.3.11.41 – Deverá permitir aplicar políticas de filtro de conteúdo Web, que seja baseado em categorias de sites automaticamente atualizadas, para todas as redes cujo tráfego seja tunelado até a Controladora;

6.3.11.42 – Deverá permitir aplicar políticas de antivírus, com detecção e bloqueio de malwares e redes botnet, entre todas as redes cujo tráfego seja tunelado até a Controladora;

6.3.11.43 – Deverá permitir aplicar políticas de IPS, bloqueando e/ou monitorando tentativas de ataques, com base de assinatura de ataques atualizada automaticamente, entre todas as redes cujo tráfego seja tunelado até a Controladora;

6.3.11.44 – Deverá permitir aplicar políticas de controle AntiSpam para todas as redes cujo tráfego seja tunelado até a Controladora;

6.3.11.45 – Deverá permitir controlar, identificar e bloquear tráfego de aplicações do tipo P2P, IM, Chat, Redes Sociais, Skype, Proxies Anônimos, streamings de áudio e vídeo, jogos entre outros, e que seja baseado no padrão de comunicação de tais aplicações, entre todas as redes cujo tráfego seja tunelado até a Controladora;

6.3.11.46 – A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede;

6.3.11.47 – Deverá possuir as seguintes certificações:

6.3.11.48 – Certificação Wi-Fi Alliance;

6.3.11.49 – Certificação ICSA para Firewall

6.3.11.50 – Certificação ICSA para Antivírus;

6.3.11.53 – Certificação ICSA para VPN SSL;

6.3.11.54 – Certificação ICSA para VPN IPSec;

6.3.11.55 – Certificação ICSA para IPS;

6.3.11.56 – O equipamento de firewall e/ou IPS deverá ter sido aprovado nos testes da NSS Labs e deverá estar na lista de recomendados.

6.3.12 – FUNCIONALIDADE DE SD-WAN

6.3.12.1 – A solução SD-WAN deve ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.

6.3.12.2 – A solução SD-WAN deve suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos.

6.3.12.3 – A solução SD-WAN deve suportar segmentação de tráfego onde seja possível aplicar políticas de IPS e Antivírus entre segmentos de LAN.

6.3.12.4 – A solução SD-WAN deve prover capacidade de inspeção SSL para a inspeção de tráfego https nas filiais, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações.

6.3.12.5 – Solução deve ser capaz de prover Zero Touch provisioning.

6.3.12.6 – A solução de Zero Touch provisioning deve ser capaz de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN.

6.3.12.7 – Solução deve ser capaz de prover uma arquitetura onde em uma comunicação Matriz x Filiais, em que a comunicação de uma Filial A para a Matriz esteja comprometida, possa ser utilizada a comunicação entre Filial B e Matriz, em que através deste circuito, a Filial A alcance a Matriz.

6.3.12.8 – A solução deve ser capaz de criar VPN "Full-Mesh" em interface gráfica ou CLI, de forma automática, e sem que o administrador precise configurar site por site.

6.3.12.9 – A configuração VPN IPSEC Deve oferecer suporte para DH Group: 14 e 15.

6.3.12.10 – Reconhecimento em camada 7 totalmente segregado da camada 4.

6.3.12.11 – Deve de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação à um determinado IP/ range de IPs de destino.

6.3.12.12 – O reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;

6.3.12.13 – Ainda sobre o reconhecimento de Aplicações, a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook, etc)

6.3.12.14 – A solução de SD-WAN deve suportar Roteamento dinâmico BGP com suporte a IPv6

6.3.12.15 – A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-

WAN em condições onde a largura de banda é modificada.

6.3.12.16 – A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN.

6.3.12.17 – A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link principal recuperado seja X% (com X variando de 10 à 50) do seu valor de saúde melhor que o link atual.

6.3.12.18 – A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorra dentro de um espaço de tempo de X segundos, configurável pelo administrador do sistema.

6.3.12.19 – A solução deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN.

6.4 – ITEM 03 – SOLUÇÃO DE ATIVOS DE REDE – SWITCH

6.4.1 – A solução deve ser composta de um único equipamento, montável em rack 19" devendo este vir acompanhado dos devidos acessórios para tal;

6.4.2 – Deve possuir, no mínimo, 24 portas GE RJ45;

6.4.3 – Deve possuir, no mínimo, 4 portas GE SFP para instalação de transceivers;

6.4.4 – Detecção automática MDI/MDIX em todas as portas UTP RJ-45.

6.4.5 – Possuir altura máxima de 1U (1,75")

6.4.6 – Implementar jumbo frames em todas as portas ofertadas, com suporte a pacotes de até 9216 Bytes.

6.4.7 – Deve possuir capacidade de vazão de ao menos 55 Gbps;

6.4.8 – Deve possuir capacidade de encaminhamento de pacotes por segundo (pps) de, no mínimo, 80 Mpps;

6.4.9 – Deve possuir tabela para 8 mil endereços MAC;

6.4.10 – Deve suportar 4 mil VLAN's 802.1q;

6.4.11 – Implementar agregação de links utilizando LACP. Deverá ser possível a formação de grupos com até 8 portas;

6.4.12 – Deve ser fornecida Solução de Gerência Centralizada de Equipamentos, caso compatível poderá ser utilizada atual solução existente na DESO, Marca Fortinet, Modelo FMG-VM.

6.4.13 – Deve ser compatível e gerenciado pelos equipamentos fornecidos dos itens 1 e 2 deste termo;

- 6.4.14 – Deve implementar 802.1s – MSTP;
- 6.4.15 – Deve implementar autenticação 802.1x;
- 6.4.16 – Deve permitir autenticação em servidores RADIUS;
- 6.4.17 – Deve implementar IP multicast;
- 6.4.18 – Deve implementar associação automática de VLAN de acordo com usuário autenticado;
- 6.4.19 – Implementar SNMPv3 e SSH;
- 6.4.20 – Deve suportar HTTP REST APIs para configuração e monitoramento;
- 6.4.21 – Implementar TFTP e FTP em IPv4;
- 6.4.22 – Implementar LLDP e LLDP-MED;
- 6.4.23 – Deve implementar recurso de proteção contra loops de rede;
- 6.4.24 – Deve implementar storm control;
- 6.4.25 – Deve implementar DHCP snooping;
- 6.4.26 – Deve implementar Dynamic ARP Inspection;
- 6.4.27 – Deve possuir fonte de alimentação com tensão 110/220VAC;
- 6.4.28 – Deve possuir pelo menos 256 MB de memória DRAM;
- 6.4.29 – Deve possuir pelo menos 32 MB de memória Flash;
- 6.4.30 – Deve possuir buffer de pacotes de, pelo menos, 512 Kbps;
- 6.4.31 – Deve implementar SNTP;
- 6.4.32 – Deve implementar os seguintes padrões IEEE: IEEE 802.1ab, IEEE 802.1D, IEEE 802.1Q, IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3u, IEEE 802.3x;
- 6.4.33 – A solução de gerência centralizada deverá atender minimamente aos itens descritos abaixo:
 - 6.4.33.1 – Permitir total configuração dos equipamentos por meio de interface WEB em IP de gerência único;
 - 6.4.33.2 – Permitir criação de vlans;
 - 6.4.33.3 – Permitir roteamento entre vlans;
 - 6.4.33.4 – Suportar IPV4 e IPV6;
 - 6.4.33.5 – Ser compatível os seguintes protocolos de prevenção de loops:
 - 6.4.33.5.1 – Spanning tree;
 - 6.4.33.5.2 – Loop guard;
 - 6.4.33.6 – Criar topologia física e lógica dos ativos de rede gerenciados de forma automática;
 - 6.4.33.7 – Dhcp snooping;

- 6.4.33.8 – Igmp snooping;
- 6.4.33.9 – Profiles LLDP;
- 6.4.33.10 – Criar políticas de QOS;
- 6.4.33.11 – Permitir visualização dos seguintes dados dos usuários por porta conectada:
 - 6.4.33.11.1 – Mac address;
 - 6.4.33.11.2 – Pacotes enviados;
 - 6.4.33.11.3 – Pacotes recebidos;
 - 6.4.33.11.1 – Vlan configurada na porta conectada;
- 6.4.34 – A CONTRATANTE deve ter acesso a todos os firmwares lançados pelo fabricante durante o período de 48 (quarenta e oito meses) através do site do fabricante;

6.5 – ITEM 04 – SOLUÇÃO DE ATIVOS DE REDE WIRELESS

- 6.5.1 – A CONTRATADA deve realizar a instalação inicial do equipamento que está restrita a entrega do equipamento, conferência de itens e teste inicial de funcionamento.
- 6.5.2 – Deve possuir, ao menos, 02 (duas) interfaces de rede 10/100/1000 Base-T RJ-45.
- 6.5.3 – Deve possuir, ao menos, 01 (uma) interface de console RS-232 RJ-45.
- 6.5.4 – Deve possuir, ao menos 01 rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento.
- 6.5.5 – Deve suportar, ao menos, 16 (dezesesseis) SSIDs simultâneos por Ponto de Acesso, sendo, pelo menos, 08 (oito) por rádio.
- 6.5.6 – Deve possuir potência de transmissão de, ao menos, 21 dBm.
- 6.5.7 – Deve possuir antenas internas e integradas com padrão de irradiação omnidirecional compatíveis com as frequências de rádio dos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax com ganhos de, no mínimo, 3 dBi para 5GHz.
- 6.5.8 – Deve suportar operação na temperatura de 0 a 40 °C.
- 6.5.9 – Deve ser fornecido com todos os acessórios necessários para que seja feita sua fixação em teto ou parede.
- 6.5.10 – Deve suportar os padrões 802.11a/b/g/n/ac/ax.
- 6.5.11 – Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;

- 6.5.12 – O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (wIDS/wIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação;
- 6.5.13 – Deve possuir a tecnologia MU-MIMO com operação 2x2.
- 6.5.14 – Deve suportar taxas de conexão (data rate) de até 1.2 Gbps.
- 6.5.15 – Deve atender aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac Wave1/Wave2 e IEEE 802.11ax, com operação nas frequências de 2.4 GHz e 5 GHz de forma simultânea
- 6.5.16 – Deve possuir PoE (Power over Ethernet), padrão 802.3at, possibilitando seu uso sem a necessidade de fontes de energia externas em qualquer porta Ethernet.
- 6.5.17 – Deverá possuir Power Injector compatível com a solução.
- 6.5.18 – Deve suportar a criação de redes mesh.
- 6.5.19 – O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser encaminhados via túnel seguro (com criptografia) até o controlador wireless;
- 6.5.20 – Deve suportar a criação de enlaces de bridge entre 02 (dois) Access Points.
- 6.5.21 – Deve suportar associação dinâmica de usuários a VLANs de acordo com parâmetros de autenticação.
- 6.5.22 – Em conjunto com o controlador wireless, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz;
- 6.5.23 – Deve possuir funcionalidade de ajuste de potência automática, de forma a reduzir interferência entre canais.
- 6.5.24 – Deve implementar UL (uplink) MU-MIMO 802.11ax mode.
- 6.5.25 – Deve implementar Spectrum Analyzer.
- 6.5.26 – Deve implementar Spatial Reuse (BSS Coloring).
- 6.5.27 – Deve suportar recurso de Target Wake Time (TWT) configurado por SSID;
- 6.5.28 – Deve possuir certificação WiFi Alliance.
- 6.5.29 – Deve possuir homologação da ANATEL, de acordo com a Resolução número 242.

6.5.30 – Deve ser compatível e gerenciado pela atual solução existente, ou por solução do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:

6.5.30.1 – Deverá ser capaz de gerenciar, de forma centralizada, outros Pontos de Acesso do mesmo fabricante;

6.5.30.2 – Deverá suportar o serviço de servidor DHCP por SSID para prover endereçamento IP automático para os clientes wireless;

6.5.30.3 – Deverá suportar monitoração e supressão de Ponto de Acesso indevido;

6.5.30.4 – Deverá prover autenticação para a rede wireless através de bases externas, como: LDAP, RADIUS ou TACACS+;

6.5.30.5 – Deverá permitir a visualização dos clientes conectados;

6.5.30.6 – Deverá prover suporte a Fast Roaming;

6.5.30.7 – Deverá ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF;

6.5.30.8 – A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;

6.5.30.9 – Deverá possuir Captive Portal por SSID;

6.5.30.10 – Deverá permitir configurar o bloqueio de tráfego entre SSIDs;

6.5.30.11 – Deverá possuir método de descoberta de novos Pontos de Acesso baseados em Broadcast ou Multicast;

6.5.30.12 – Deverá possuir lista contendo Pontos de Acesso Aceitos e Pontos de Acesso Indevidos (Rogue);

6.5.30.13 – Deverá possuir controle baseado em política de firewall para acesso entre as WLANs cujo tráfego seja tunelado até a Controladora;

6.5.30.14 – Deverá permitir a criação de políticas de traffic shaping entre todas as redes cujo tráfego seja tunelado até a Controladora;

6.5.30.15 – Deverá permitir a criação de políticas de firewall baseadas em horário;

6.5.30.16 – Deverá permitir NAT nas políticas de firewall;

6.5.30.17 – Deverá possibilitar definir número de clientes por SSID;

6.5.30.18 – Deverá permitir e/ou bloquear o tráfego entre SSIDs;

6.5.30.19 – Deverá possuir mecanismo de criação automática de usuários visitantes e senhas autogeradas

e/ou manual, que possam ser enviadas por e-mail ou SMS aos usuários, e com capacidade de definição de horário da expiração da senha;

6.5.30.20 – A comunicação entre o Access Point e a Controladora Wireless deverá poder ser efetuada de forma criptografada;

6.5.30.21 – Deverá possuir mecanismo de ajuste de potência do sinal, de forma a reduzir interferência entre canais entre 02 (dois) Access Points gerenciados;

6.5.30.22 – Deverá possuir mecanismo de balanceamento de tráfego/usuários entre Access Points;

6.5.30.23 – Deve possuir mecanismo de balanceamento de tráfego/usuários entre frequências e/ou rádios;

6.5.30.24 – Toda a configuração do Ponto de Acesso deverá ser executada através da Controladora Wireless;

6.5.30.25 – Deverá permitir a identificação de APs com firmware desatualizado e efetuar o upgrade via interface gráfica;

6.5.30.26 – Deverá possuir console de monitoramento dos usuários conectados, indicando em que Access Point, em que rádio, em que canal, endereço IP do usuário, tipo de dispositivo e sistema operacional, uso de banda, potência do sinal e relação sinal/ruído;

6.5.30.27 – Deverá permitir aplicar políticas de IPS, bloqueando e/ou monitorando tentativas de ataques, com base de assinatura de ataques atualizada automaticamente, entre todas as redes cujo tráfego seja tunelado até a Controladora;

6.5.30.28 – Deve suportar Wi-Fi Protected Access (WPA), WPA2 ou WPA3 por SSID, utilizando-se de AES e/ou TKIP;

6.5.30.29 – Deve suportar os seguintes métodos de autenticação EAP:

6.5.30.29.1. EAP-TLS , EAP-TTLS, EAP-PEAP, EAP-SIM, EAP-AKA;

6.5.30.30 – Deve suportar 802.1x através de RADIUS;

6.5.30.31 – Deve suportar filtro baseado em endereço MAC por SSID;

6.5.30.32 – Deve permitir configurar parâmetros de rádio, como: banda e canal;

6.5.30.33 – Deve possuir método de descoberta de novos Pontos de Acesso baseados em Broadcast ou Multicast;

6.5.30.34 – Deve possuir mecanismo de identificação e controle de Rogue APs, suportando supressão automática e bloqueio por endereço MAC de APs;

6.5.30.35 – Deve possuir lista contendo Pontos de Acesso Aceitos e Pontos de Acesso Indevidos (Rogue);

6.5.30.36 – Deve possuir WIDS com, ao menos, os seguintes perfis:

6.5.30.36.1 – Rogue/Interfering AP Detection;

6.5.30.36.2 – Ad-hoc Network Detection;

6.5.30.36.3 – Wireless Bridge Detection;

6.5.30.36.4 – Weak WEP Detection;

6.5.30.36.5. MAC OUI Checking;

6.5.30.37 – A solução Deve detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm;

6.5.30.38 – O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser encaminhados dentro do túnel até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional do próprio fabricante para suportar a conexão dos túneis originados dos pontos de acesso;

6.5.30.39 – Deverá possuir as seguintes certificações:

6.5.30.39.1 – Certificação Wi-Fi Alliance;

6.5.30.39.2 – Certificação ICSA para VPN SSL;

6.5.30.39.3 – Certificação ICSA para VPN IPSec;

6.5.30.39.4 – Certificação ICSA para IPS;

6.5.31 – A CONTRATANTE deve ter acesso a todos os firmwares lançados pelo fabricante durante o período de 48 (quarenta e oito meses) através do site do fabricante;

6.6 – ITEM 05 – SOLUÇÃO PARA DUPLO FATOR DE AUTENTICAÇÃO – TIPO I

6.6.1 – Deve possuir 10 (dez) licenciamentos perpétuos de token e sem limites de transferência para outros dispositivos;

6.6.2 – Deve permitir o download gratuito nas lojas de aplicativos separado do seu provisionamento;

6.6.3 – O aplicativo deve suportar exclusão e adição de novos tokens;

6.6.4 – Deve ser instalado no dispositivo móvel sem que haja a necessidade de alteração de sua configuração, ou mesmo a capacidade de formatar o dispositivo móvel de forma remota;

6.6.5 – Deve garantir a privacidade do dispositivo móvel, ou seja, não deve ser capaz de consultar histórico de navegação;

6.6.6 – Deve requerer a permissão proprietário para envio de notificações ou qualquer tipo de alteração nas configurações;

- 6.6.7 – Deve suportar as principais plataformas de mobile do mercado (iOS (iPhone, iPod Touch, iPad), Android, Windows Phone 8, 8.1, Windows 10 ou superior);
- 6.6.8 – Deve suportar a geração dinâmica das sementes de token, minimizando a exposição online;
- 6.6.9 – Deve suportar ativação através da utilização de QR Codes e manual;
- 6.6.10 – Deve criptografar o armazenamento de sementes utilizadas na geração do token;
- 6.6.11 – Deve ser capaz de gerar senhas de uso único (One Time Programmable - OTP) baseado em tempo (TOTP) ou evento (HTOP) compatível com OATH;
- 6.6.12 – Deve suportar a ocultação do token para tokens baseados em tempo (TOTP);
- 6.6.13 – Deve capaz de proteger abertura do aplicativo através de PIN ou Impressão Digital ou Face Security;
- 6.6.14 – Deve exibir o intervalo de tempo OTP;
- 6.6.15 – Deve exibir do número de série do token;
- 6.6.16 – Deve ser compatível com o relógio da Apple;
- 6.6.17 – Deve suportar que a senha gerada possa ser copiada para a área de transferência;
- 6.6.18 – Deve suportar detalhes de login enviados ao telefone para aprovação com um toque;
- 6.6.19 – Deve usar um serviço de provisionamento dinâmico, onde apenas na atribuição de um token a um usuário a semente é criada e é removida durante o download ou após um tempo limite configurável;
- 6.6.20 – Deve ser compatível e integrável com a solução de segurança de rede NGFW, já existente na DESO, Fortigate 200F do fabricante Fortinet;
- 6.6.21 – Deve estar de acordo com as seguintes RFCs para especificações OTP: RFC6238 e RFC4226;
- 6.6.22 – Deve ser capaz de realizar vinculação com o dispositivo móvel;
- 6.6.23 – Deve suportar à sua utilização como segundo fator de autenticação para acesso VPN via SSL ou IPSEC, sem a necessidade de utilização de um servidor Radius;
- 6.6.24 – Deve ser compatível com Google, Dropbox, Amazon e outros tokens TOTP (Time-based One-Time Password) compatíveis com OAT;

6.7 – ITEM 06 – SOLUÇÃO PARA DUPLO FATOR DE AUTENTICAÇÃO – TIPO II

- 6.7.1 – Deve possuir 10 (dez) dispositivos de autenticação multifator (MFA);
- 6.7.2 – Deve ter capacidade de distribuir as chaves criptográficas dos tokens, além de permitir a configuração de políticas de segurança;
- 6.7.3 – Deve ter Display LCD de 6 dígitos para exibição do código de autenticação;
- 6.7.4 – A bateria deve ter uma duração de tempo igual à garantia exigida para o equipamento;

- 6.7.5 – Deve possuir licença perpétua;
- 6.7.6 – Deve suportar ativação através da utilização de QR Codes e manual;
- 6.7.7 – Deve ser resistente a água;
- 6.7.8 – Deve ser capaz de gerar senhas de uso único (One Time Programmable - OTP) baseado em tempo (TOTP) compatível com OATH;
- 6.7.9 – Deve suportar a ocultação do token para tokens baseados em tempo (TOTP);
- 6.7.10 – Deve exibir o intervalo de tempo OTP;
- 6.7.11 – Deve possuir certificado FIPS 140-2;
- 6.7.12 – Deve ser compatível e integrável com a solução de segurança de rede NGFW, já existente na DESO, Fortigate 200F do fabricante Fortinet;
- 6.7.13 – Deve estar de acordo com as seguintes RFCs para especificações OATH-TOTP: RFC6238;
- 6.7.14 – Deve possuir certificação de hardware (RoHS, CE, FCC, ICES, UKCA Compliant);
- 6.7.15 – Deve suportar à sua utilização como segundo fator de autenticação para acesso VPN via SSL ou IPSEC, sem a necessidade de utilização de um servidor Radius;
- 6.7.16 – Deve ser compatível com Google, Dropbox, Amazon e outros tokens TOTP (Time-based One-Time Password) compatíveis com OAT;
- 6.7.17 – A CONTRATANTE deve ter acesso a todos os firmwares lançados pelo fabricante, se houver, durante o período de 48 (quarenta e oito meses) através do site do fabricante;

6.8 – IMPLANTAÇÃO E SUPORTE TÉCNICO

Após as entregas dos equipamentos/solução especificados nos itens 1 a 6 a CONTRATADA ficará responsável pela implantação, configuração e testes dos equipamentos.

- 6.8.1 – O serviço deve ser prestado pelo próprio fabricante (Professional Services) ou pela empresa contratada.
- 6.8.2 – Atividades: assessoria; desenvolvimento de plano de implementação; planejamento; análise; configuração; integração; migração; testes de verificação; ajustes; otimização; troubleshooting; updates; upgrades; provas de conceito; ensaios de contingência; customização de consultas de relatórios; treinamentos "hands-on"; análise de vulnerabilidades; criação e manutenção de regras de segurança e redes; participação em comitês de segurança para esclarecimentos; documentação "as built"; documentação para rollout;
- 6.8.3 – Os perfis dos profissionais/atividades definidas seguirão o padrão de perfis indicados por

metodologias de projetos, como PMBOK. Abaixo, um detalhamento sobre os perfis de profissionais e o escopo de cada um de seus papéis:

6.8.4 – Arquitetura: definição da arquitetura lógica e física do projeto, garantindo a qualidade durante a implantação e o atendimento de todos os requisitos funcionais e não funcionais; propor melhorias; definir controles e monitoramento do ambiente, sugerindo métricas, thresholds e indicadores de acompanhamento; apoio no planejamento, execução e avaliação de mudanças;

6.8.5 – Implementação: Levantamento de dados, execução das implantações incluindo configuração customizada, integração, migrações e testes, adaptações código, criação de infraestrutura, orientação, documentação etc.;

6.8.6 – Gerenciamento de projetos: gerenciamento do projeto propriamente dito, considerando controle de prazos, esforço, elaboração de relatórios de posicionamento executivo, indicadores do projeto e qualquer outra métrica prevista no PMBOOK. O objetivo de todas estas atividades é a garantia de qualidade do projeto no que tange prazos e esforço

6.8.7 – Suporte: Atendimento a incidentes de suporte realizando análises, troubleshooting, diagnósticos; realizando ajustes e otimização configurações; analisando e aplicando patches, fixes e updates, aplicando testes e realizando ensaios; monitorando o ambiente;

6.8.8 – As atividades deverão ser prestadas na modalidade on-site, exceto quando expressamente autorizado pela CONTRATANTE;

6.8.9 – A CONTRATADA deve nomear funcionário capacitado que será responsável por fornecer aconselhamento técnico e operacional sobre os serviços; assistência sobre as condições do contrato; gerenciamento de escalação junto ao Fabricante; Gerenciamento de recursos e cronograma de entrega dos serviços;

6.8.10 – Neste modelo de execução dos serviços não se caracteriza a subordinação direta e nem a pessoalidade, visto que não haverá qualquer relação de subordinação jurídica entre os profissionais da equipe da empresa contratada e este Órgão. As empresas proponentes deverão considerar em seus custos todos os recursos necessários ao completo atendimento aos objetos, tais como despesas com pessoal (salários, férias, encargos, benefícios, seleção, outras) de modo a garantir os serviços definidos;

7 – LOCAL E PRAZO DE ENTREGA

O objeto será fornecido de acordo com as quantidades solicitadas com base nas Ordens de Serviços emitidas, correndo o frete, a carga e o transporte do produto às expensas do fornecedor. As entregas

ocorrerão mediante programação e conforme as necessidades da DESO.

7.1. LOCAL DE ENTREGA

Os itens licitados deverão ser entregues no seguinte endereço: **GTIC – Gerência de Tecnologia da Informação e Comunicação, localizada na Sede da DESO, Rua Campo Do Brito, No 331, Bairro Praia 13 de Julho, Aracaju/SE**, nos seguintes horários: 07h:00 às 12h:00 e das 14h:00 às 16h:00;

7.1.1. Prazo de entrega: A CONTRATADA deve realizar a entrega, instalação e todas as configurações dos equipamentos em até 90 (noventa) dias, contados da data de assinatura do Contrato, iniciando neste momento a prestação dos serviços objetos desta contratação.

8 – INSTALAÇÃO, GARANTIA, SUPORTE E TESTES

8.1. A CONTRATADA deverá disponibilizar a instalação inicial de todos os equipamentos solicitados bem como a garantia do fabricante que deve ser de 48 (quarenta e oito) meses e treinamento de acordo com os demais itens deste Termo de Referência, uma equipe com perfil técnico adequado as atividades previstas, com técnicos treinados pelo fabricante para a operação e configuração de todos os componentes ofertados.

8.2. Os chamados de suporte deverão ser abertos diretamente na CONTRATADA, gerenciados pelo mesmo, através de número telefônico 0800 ou equivalente a ligação local e/ou por ambiente WEB, fornecendo, neste momento, o número, data e hora de abertura do chamado. Este será considerado o início para contagem dos prazos estabelecidos.

8.3. Durante todo o período de garantia contratado, o serviço de suporte deve ser suprido 24 (vinte e quatro) horas, 07 (sete) dias por semana.

8.4. A CONTRATADA deve disponibilizar acesso ao ambiente WEB do fabricante para download de arquivos, drivers e firmwares.

8.5. Todo serviço de suporte deve ser realizado por profissional certificado pelo fabricante.

8.6. O serviço de suporte deve proporcionar a interação com a equipe técnica da CONTRATANTE, fornecendo apoio na resolução de incidentes que envolvam os componentes da oferta, garantindo seu pronto reestabelecimento.

9 – DAS OBRIGAÇÕES DAS PARTES

9.1 – DA CONTRATADA

- 9.1.1 – Entregar os produtos e serviços cumprindo rigorosamente todas as especificações, prazos, obrigações e cláusulas estabelecidas neste edital e seus Anexos;
- 9.1.2 – Zelar pela perfeita execução do contrato;
- 9.1.3 – Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas no ato convocatório;
- 9.1.4 – Responsabilizar-se pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do contrato, obrigando-se a liquidá-los nos respectivos vencimentos, sabendo que:
- 9.1.4.1 – A inadimplência do contratado, com referência aos encargos trabalhistas, fiscais, previdenciários e comerciais não transfere à Administração Pública a responsabilidade por seu pagamento, nem poderá onerar o objeto do contrato; e
- 9.1.4.2 – Não existirá, em hipótese alguma, nenhum vínculo empregatício entre os empregados da Contratada e a Contratante.
- 9.1.5 – Responsabilizar-se por quaisquer danos pessoais e/ou materiais, causados por seus empregados diretamente à Administração ou a terceiros, decorrentes de sua culpa ou dolo na execução do contrato, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pela contratante;
- 9.1.6 – Responsabilizar-se por todos os encargos e obrigações previstos na legislação pertinente a acidentes de trabalho, quando forem vítimas os seus funcionários no desempenho dos serviços objeto desta licitação, mesmo que ocorrido nas dependências da Contratante, assim como pelos seguros e demais obrigações empregatícias vigentes e futuras;
- 9.1.7 – Responsabilizar-se pelas eventuais despesas para execução do serviço solicitado, qualquer que seja o valor.
- 9.1.8 – Não transferir a qualquer título, os serviços contratados;
- 9.1.9 – Independentemente de transcrição na proposta, sujeitar-se às demais obrigações estabelecidas neste Termo de Referência.
- 9.1.10 – Cumprir todas as especificações, obrigações e cláusulas estabelecidas no Edital e seus Anexos;
- 9.1.11 – Comunicar à contratante, por escrito, qualquer anormalidade de caráter urgente e prestar, com a devida antecedência, os esclarecimentos necessários;
- 9.1.12 – Assumir inteira responsabilidade sobre o objeto contratado perante a DESO;
- 9.1.13 – Providenciar a imediata correção das deficiências, falhas ou irregularidades apontadas pela Contratante na execução do objeto, atendendo às solicitações do executor do contrato, voltadas ao saneamento e correção da(s) irregularidade(s) verificada(s);

9.2. DA DESO

9.2.1 – Proporcionar à CONTRATADA todas as facilidades para que possa desempenhar o objeto do Termo de Referência de forma satisfatória.

9.2.2 – Designar uma equipe técnica para fiscalizar e acompanhar a execução dos serviços prestados.

9.2.3 – Avaliar e aprovar a execução dos serviços, funcionalidades da solução e a qualidade do projeto, solicitando à CONTRATADA a correção das não conformidades, sem que haja ônus para a DESO.

9.2.4 – Prestar as informações e os esclarecimentos que venham a ser solicitados pelos responsáveis da CONTRATADA.

9.2.5 – Dar ciência à CONTRATADA de quaisquer modificações que venham a ocorrer.

9.2.6 – Atestar as notas fiscais/faturas, por unidade competente, emitidas pela CONTRATADA, recusando-as quando inexatas ou incorretas, efetuando todos os pagamentos nas condições pactuadas.

10 – DA GESTÃO E FISCALIZAÇÃO

10.1. Gestor do Contrato

10.1.1. É de responsabilidade do ocupante da função FG-5 da Gerência de Tecnologia da Informação e Comunicação – GTIC a gestão do contrato;

10.1.2. É de responsabilidade do gestor do contrato:

- a) Aplicar sanções e glosas mediante indicação do fiscal do contrato;
- b) Liberação de pagamento mediante autorização do fiscal do contrato, após conferência da entrega em conformidade do produto ao especificado neste termo;

10.2. Fiscal do Contrato

10.2.1. É de responsabilidade do ocupante da função FG-4 da Coordenação de Infraestrutura – CINF a fiscalização do contrato;

10.2.2. É de responsabilidade do fiscal do contrato:

- a) Avaliação da qualidade do produto;
- b) Identificação de não conformidade do produto entregue e notificação ao gestor do contrato;
- c) Autorização para faturamento mediante conferência da entrega em conformidade do produto ao especificado neste termo;

11 – DO PAGAMENTO

11.1. O pagamento deverá ser efetuados em até 30 (trinta) dias após a apresentação de fatura com os quantitativos entregues. Todas com o atesto do fiscal do contrato.

11.2. Serão pagos apenas os valores relativos aos quantitativos entregues, conforme quantidade solicitada e atendimento as especificações descritas neste Termo de Referência.

11.3. Nenhum pagamento será efetuado a empresa, enquanto houver pendência de liquidação de obrigação financeira, em virtude de penalidade ou inadimplência contratual.

11.4. Caso se faça necessária a apresentação ou reapresentação de qualquer Nota Fiscal/Fatura ou documentação por culpa da contratada, o prazo de até 30 (trinta) dias reiniciar-se-á a contar da data da respectiva apresentação ou reapresentação.

12 – DAS DISPOSIÇÕES GERAIS

A DESO realizará uma reunião de integração com o Fornecedor antes da assinatura do contrato.

A CONTRATADA deverá assumir todos os custos, ônus e taxas, decorrentes do fornecimento, devendo ser previamente verificados pela empresa em sua proposta comercial. Não serão aceitos custos adicionais sob qualquer pretexto, devendo a empresa dirimir previamente todas as dúvidas e assumir inteira responsabilidade pelo fornecimento do objeto.

O adequado transporte para entrega dos materiais, no local indicado, data e prazos de fornecimento são de integral responsabilidade da CONTRATADA.

Todos os equipamentos a serem fornecidos deverão ser novos, não reconicionados e/ou remanufaturados, sem qualquer uso anterior.

13 – DISPOSIÇÕES ESPECÍFICAS

13.1 – OS RECURSOS ORÇAMENTÁRIOS:

Os recursos para o pagamento dos serviços objeto do Pregão Eletrônico, provêm da previsão de Recursos Próprios da DESO, constante do Orçamento para o exercício de 2023 e 2024.

13.2 – CLASSIFICAÇÃO ORÇAMENTÁRIA

As despesas decorrentes do objeto desta licitação obedecerão a classificação adiante discriminada, consignada no orçamento empresarial da DESO.

Conta: 400.03 – BENS E EQUIPAMENTOS

13.3 – VALIDADE DA PROPOSTA

O prazo de validade da proposta não pode ser inferior a 60 (sessenta) dias consecutivos, contados

da data da sessão pública de abertura desta licitação.

13.4 – DA SUBCONTRATAÇÃO E ALTERAÇÃO SUBJETIVA

13.4.1 – Não será admitida a subcontratação do objeto licitatório.

13.4.2 – É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

13.5 – PRAZO DE VIGÊNCIA

O prazo de vigência contratual será de 48 (quarenta e oito) meses.

13.6 – DO CRITÉRIO DE JULGAMENTO

O critério de julgamento será o de MENOR PREÇO DO LOTE

13.7 – DO REGIME DE EXECUÇÃO

O regime de execução será por PREÇO UNITÁRIO.

14 – DAS CONDIÇÕES DE PARTICIPAÇÃO

14.1 – Poderão participar do certame todos os interessados do ramo de atividade pertinente ao objeto da contratação.

14.2 – Não poderão participar os interessados que se encontrarem sob falência, concurso de credores, dissolução, liquidação, empresas estrangeiras que não funcionam no país, nem aqueles que tenham sido declarados inidôneos para licitar ou contratar com a Administração Pública, ou punidos com suspensão do direito de licitar e contratar com a DESO.

14.3 – A participação neste certame implica aceitação de todas as condições estabelecidas neste instrumento.

14.4 – Não será admitida a participação de empresas reunidas em consórcios para fornecimento dos produtos e/ou serviços necessários à composição da solução, de acordo com as exigências previstas no Edital e seus anexos.

15 – DAS SANÇÕES ADMINISTRATIVAS

15.1 – A contratada pelo inadimplemento de suas obrigações, garantida a prévia defesa da CONTRATADA no prazo de 10 (dias) dias úteis, ficará sujeita as seguintes sanções previstas no RILC e na Lei 13.303/2016:

15.1.1 – Advertência;

15.1.2 – Multa moratória;

15.1.3 – Multa compensatória;

15.1.4 – Suspensão do direito de participar de licitação e impedimento de contatar com a DESO, pelo prazo de até 02 (dois) anos;

15.1.5 – Declaração de inidoneidade para licitar ou contratar com a Administração Pública.

15.2 – As sanções constantes no subitem 15.1 poderão ser aplicadas de forma cumulativa.

15.3 – Ficar impedida de licitar e de contratar com a Administração Pública Estadual, pelo prazo de até 05 (cinco) anos, garantido o direito prévio de defesa, o fornecedor que:

15.3.1 – Ensejar o retardamento da execução do objeto desta licitação;

15.3.2 – Não mantiver proposta, injustificadamente;

15.3.3 – Comportar-se de modo inidôneo;

15.3.4 – Fizer declaração falsa;

15.3.5 – Cometer fraude fiscal;

15.3.6 – Falhar ou fraudar no fornecimento do objeto.

15.4 – São consideradas condutas reprováveis e passíveis de sanções, dentre outras, as previstas no art. 186 do RILC.

15.5 – As multas estabelecidas serão entendidas como independentes e cumulativas e serão compensadas pela DESO com as importâncias em dinheiro, relativas às prestações a que corresponderem, ou da garantia do contrato, quando for o caso, cobradas judicialmente.

15.6 – A aplicação de sanção de advertência se efetiva com o registro da mesma junto ao cadastro de fornecedores e no sistema de gerenciamento de contatos da DESO, independentemente de tratar-se de pessoa cadastrada ao não.

15.7 – A multa poderá ser aplicada nos seguintes casos:

I – Em decorrência da interposição de recursos meramente procrastinatórios, poderá ser aplicada multa correspondente 3% do valor máximo estabelecido para a licitação em questão.

II – Em decorrência da não regularização da documentação de habilitação, nos termos do artigo 43, § 1º da Lei Complementar nº 123/2006, a vista do subitem 15.3.6, poderá ser aplicada multa correspondente 3% do valor máximo estabelecido para a licitação em questão.

III – Pela recusa em assinar o contrato, aceitar ou retirar o instrumento equivalente, dentro do prazo estabelecido por este edital, poderá ser aplicada multa correspondente a 5% do valor máximo estabelecido para a licitação em questão.

IV – No caso de atraso na entrega da garantia contratual, quando exigida, o instrumento convocatório deverá prever, mediante competente justificativa, a incidência de multa correspondente 3% do valor total do contrato;

V – No caso de inexecução parcial, incidirá multa na razão de 10% sobre o valor da parcela não executada;

VI – No caso de inexecução total, incidirá multa na razão de 25% sobre o saldo remanescente do contrato;

VII – nos demais casos de atraso, incidirá multa na razão de 5% sobre o valor da parcela em atraso.

15.8 – Caso não haja o recolhimento da multa no prazo estipulado, a DESO descontará a referida importância de eventuais créditos a vencer da empresa contratada. Na ausência de créditos disponíveis para quitação da importância da multa, a DESO executará a garantia quando exigida, e quando for o caso, será cobrada judicialmente.

15.9 – A DESO poderá quando do não pagamento da multa pela Contratada, aplicar a sanção de suspensão do direito de participar de licitação e impedimento de contratar com a DESO, por até 02 (dois) anos;

15.10 – Cabe a sanção de suspensão em razão de ação ou omissão capaz de causar, ou que tenha causado dano à DESO, suas instalações, pessoas, imagem, meio ambiente ou a terceiros, aplicando a disposição do art. 189 e 190 do RILC em face da legislação previdenciária, social ou trabalhista.

16 – QUALIFICAÇÃO ECONÔMICA

16.1. A licitante deverá apresentar Balanço Patrimonial e demonstrações contábeis da seguinte forma:

- a) Para as Sociedades anônimas, mediante cópia autenticada da publicação em Diário Oficial.
- b) Para as demais empresas, cópias legíveis e autenticadas das páginas do Livro Diário, onde foram transcritos o Balanço Patrimonial e a demonstração do Resultado do último exercício social, com os respectivos termos de abertura e encerramento registrados na Junta Comercial ou no Cartório de Títulos e Documentos.
- c) Para as empresas constituídas há menos de um ano, será exigido apenas o Balanço de Abertura e demonstrações contábeis na forma da lei.
- d) A capacidade econômico-financeira será verificada através de:

- Liquidez Geral: > 1

$$LG = (\text{Ativo Circulante} + \text{Realizável a Longo Prazo}) / (\text{Passivo Circulante} + \text{Passivo Circulante})$$

- Liquidez Corrente: > 1

$$LC = \text{Ativo Circulante} / \text{Passivo Circulante}$$

- Solvência Geral: > 1

$$EG = \text{Ativo Circulante} / \text{Passivo Circulante}$$

e) O Patrimônio Líquido mínimo exigido será R\$ 300.000,00, devendo a comprovação ser feita relativamente à data da apresentação da proposta.

17 – DA GARANTIA CONTRATUAL

17.1 – A empresa CONTRATADA, para garantia da execução do Contrato, apresentará na 5.0.08.00/GFIN – Gerência Financeira e Contábil desta Companhia, no prazo de 20 (vinte) dias da emissão da Ordem de Fornecimento, a importância correspondente a 3% (Três por cento) do valor Contratual, em uma das seguintes modalidades:

- a) Caução em Dinheiro;
- b) Seguro-Garantia;
- c) Fiança Bancária.

17.2 – Caso a Garantia prestada pela CONTRATADA seja em moeda corrente, será depositada em Conta a ser indicada pela DESO, a fim de se manter sua atualização financeira.

17.3 – A garantia prestada nas modalidades de Seguro-Garantia ou Fiança Bancária, deverá ser apresentada com validade de 03 meses após o término da vigência contratual.

17.4 – Fica estabelecido que a Garantia prestada não poderá ser parcelada nas faturas pagas à CONTRATADA.

17.5 – Se, por qualquer razão, durante a execução do objeto, for necessária a prorrogação do prazo de execução do Contrato, a CONTRATADA ficará obrigada a providenciar a renovação da garantia, nos mesmos termos e condições originalmente aprovados pela DESO.

17.6 – Se, no decorrer da execução do Contrato, a CONTRATADA solicitar a substituição da garantia prestada, a área gestora do Contrato deverá justificar a conveniência da substituição.

17.7 – A Garantia responderá pelo inadimplemento das condições contratuais, pela não conclusão ou conclusão incompleta dos serviços e pelas eventuais multas aplicadas, independentemente de outras cominações legais, quando for o caso.

17.8 – No caso das rescisões a devolução da Garantia somente se procederá depois de observado o art.182 §3º, e o art.183, incisos II e III do RILC.

17.9 – A garantia prestada pela CONTRATADA, será liberada pelo 5.0.08.00/GFIN, após emissão do “TERMO DE RECEBIMENTO DO MATERIAL”.

17.10 – Cessará a guarda das Garantias que não forem resgatadas pela CONTRATADA, no prazo de 60 (sessenta) dias após sua liberação, cabendo a DESO a inutilização das mesmas.

18 – CRITÉRIOS DE ACEITABILIDADE DOS PREÇOS

18.1 – Os preços unitários e global somente serão aceitos quando não superiores aos estimados no preço de referência da DESO;

18.2 – Em hipótese alguma será aceito aumento dos valores inicialmente propostos;

18.3 – Não havendo por parte do arrematante a revisão de sua proposta dentro do prazo estabelecido pelo pregoeiro, a mesma terá sua proposta desclassificada;

19 – DA PROPOSTA DE PREÇOS

19.1 – A LICITANTE deve apresentar os seguintes documentos:

19.1.1 – Prospecto com as características técnicas de todos os componentes dos equipamentos, incluindo especificação de marca, modelo e outros elementos que, de forma inequívoca, identifiquem e comprovem as configurações cotadas, possíveis expansões e upgrades, através de certificados, manuais técnicos, folders e demais literaturas técnicas editadas pelos fabricantes. Serão aceitas cópias das especificações obtidas em websites dos fabricantes na Internet, em que conste o respectivo endereço eletrônico;

19.1.2 – Indicação exata do modelo de equipamento ofertado, no Sistema Eletrônico de Disputas e na Proposta de Preços, sendo os respectivos catálogos obrigatoriamente de domínio público, ou seja, Deverão estar publicados no website do fabricante, comprovando todos os recursos e funcionalidades mínimas exigidas para os equipamentos que irão integrar as características técnicas solicitadas no item 6 deste Termo de Referência.

19.1.3 – Indicação de site na WEB para transferência de arquivos de configuração (manuais e atualizações de firmware);

19.2 – A licitante deverá estar ciente e levar em consideração, além das especificações e condições estabelecidas no Edital, o atendimento dos seguintes requisitos:

19.2.1 – Nos preços propostos deverão estar inclusos todos os custos necessários para o atendimento do objeto da licitação, bem como todos os materiais, equipamentos, impostos, encargos trabalhistas,

previdenciários, fiscais, comerciais, taxas, deslocamentos de pessoal, treinamento, garantia, montagem e instalação e quaisquer outros que incidam ou venham a incidir sobre o objeto licitado constante da proposta;

19.2.2 – Os preços deverão ser cotados em moeda corrente nacional e neles deverão estar inclusas todas e quaisquer despesas, tais como: IPI e demais impostos, encargos sociais, seguros, taxas, tributos diretos e indiretos incidentes sobre o fornecimento dos materiais;

19.2.3 – A proposta entregue será considerada com prazo de validade de 60 dias, contados da data da sessão pública de abertura desta licitação;

19.3 – Serão desclassificadas as propostas:

a) que não atendam às exigências do ato convocatório ou que apresentem dispositivos contrários à lei e à regulamentação vigente;

b) que contiverem preços ou vantagens de qualquer natureza ou descontos não previstos neste Pregão, inclusive financiamentos subsidiados ou a fundo perdido;

c) que forem omissas, vagas, apresentarem irregularidades ou defeitos capazes de dificultar o julgamento, bem como as que apresentarem preços ou vantagens baseadas nas ofertas de outros licitantes;

d) que forem superiores ao valor orçado pela DESO.

19.4 – A proposta deverá limitar-se ao objeto desta licitação, sendo desconsideradas quaisquer alternativas de preço ou qualquer outra condição não prevista.

19.5 – Independentemente de declaração expressa, a simples apresentação das propostas implica submissão a todas as condições estipuladas no Edital e seus Anexos, sem prejuízo da estrita observância das normas contidas na legislação mencionada no preâmbulo do Edital.

19.6 – A Proposta de Preço será considerada completa e abrangerá todos os custos necessários ao objeto.

19.7 – Empresas que participarem deste processo, que praticarem, injustificadamente, ato ilegal tipificado no art. 7º da Lei 10.520/2002, a Administração instaurará processo administrativo para apurar as condutas das empresas (TCU – Acórdão nº 754/2015 – Plenário) concomitantemente com as Sanções Administrativas previstas no item 14 deste Termo de referência.

Aracaju, 1 de junho de 2023



ASSINADO ELETRONICAMENTE
Verificar autenticidade conforme mensagem
apresentada no rodapé do documento

Jessica da Silva Santos
Colaborador(a)



ASSINADO ELETRONICAMENTE
Verificar autenticidade conforme mensagem
apresentada no rodapé do documento

Ronaldo Moreira de Melo Junior
Gerente

Protocolo de Assinatura(s)

O documento acima foi proposto para assinatura digital. Para verificar as assinaturas acesse o endereço <http://edocsergipe.se.gov.br/consultacodigo> e utilize o código abaixo para verificar se este documento é válido.

Código de verificação: VCOJ-KR44-RJBF-9OWN



O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 12/06/2023 é(são) :

- Jessica da Silva Santos - 01/06/2023 12:21:16
- Ronaldo Moreira de Melo Junior - 01/06/2023 11:32:51