Anexo I

TERMO DE REFERÊNCIA

1. OBJETO

1.1. **Registro de preços para aquisição de Solução de comunicação (roteadores, licenças e serviço)** visando atender às necessidades deste Tribunal Regional Eleitoral do Paraná, conforme especificações descritas no presente Termo de Referência.

1.1.1. Faz parte dos itens a serem adquiridos (itens 1, 2, 8 e 9) o fornecimento de Garantia "on site" de 24 (vinte e quatro) meses iniciada a partir do recebimento definitivo pelo gestor da contratação.

1.2. Da justificativa para a contratação:

1.2.1. A rede da Justiça Eleitoral (JE) no Paraná interliga os 156 (cento e cinquenta e seis) Fóruns Eleitorais espalhados pelo estado ao edifício sede do TRE-PR e ao TSE, possibilitando o acesso aos sistemas administrativos, instalados no TRE-PR, e aos sistemas eleitorais, instalados no TSE, necessários para o atendimento aos eleitores em todas as unidades bem como a conexão das estações de trabalho com a rede mundial de computadores.

1.2.2. Em 2017, para maximizar o tempo de disponibilidade da rede e dos sistemas, a exemplo do que já existia na conexão entre TRE e TSE, foi implantada redundância dos links de comunicação entre o TRE-PR e os Cartórios Eleitorais do estado. Para tanto, foi instalado um segundo circuito de comunicação e equipamentos de rede (roteadores) capazes de monitorar os caminhos de rede disponíveis e substituir os roteadores em uso.

1.2.3. Estes equipamentos, que sustentam esta rede, foram adquiridos com 24 (vinte e quatro) meses de garantia e este prazo está chegando ao fim. Desta forma, faz-se necessário renovar a garantia dos equipamentos para manter a disponibilidade do ambiente e também permitir a aplicação de correções e atualizações do firmware instalado, corrigindo eventuais vulnerabilidades.

1.2.4. Também é necessário considerar que o contrato 01/2018, que viabilizou a redundância da rede com a contratação de um segundo circuito de comunicação, se encerrará no primeiro semestre de 2023. Embora sejam contratações distintas, é imprescindível prever neste processo a possibilidade de implantação de licenças avançadas (tipo UTM) que permitam a ativação de funcionalidades avançadas nos roteadores, permitindo substituir circuitos MPLS do contrato 01/2018 por circuitos IP.

1.2.5. A presente aquisição se destina a aquisição de equipamentos, software e serviços para permitir a manutenção e evolução da solução de comunicação para interligação dos Cartórios Eleitorais e do Edifício Sede do Tribunal Regional Eleitoral do Paraná. Desta forma,

considerando a evolução das tecnologias e as demais necessidades do TRE-PR, faz-se necessário efetuar a renovação do licenciamento atual, de forma manter a disponibilidade da rede de comunicação e permitir a evolução deste ambiente.

1.3. Da justificativa para a exigência de marca: A presente contratação trata da aquisição de equipamentos de comunicação, de alta complexidade, visando evolução e continuidade da rede de dados iniciada em 2020 pelo pregão 60/2020. Neste pregão inicial não foi exigida marca, venceu o licitante que apresentou o menor preço para a solução. **A exigência de marca do presente pregão (Fortinet)** visa garantir a compatibilidade dos equipamentos a serem adquiridos e o ambiente já implantado, proteger do investimento já efetuado, dar padrão de funcionamento à rede e minimizar as necessidades de treinamento das equipes técnicas e usuários.

2. DOS QUANTITATIVOS A SEREM ADQUIRIDOS

2.1. A contratação será realizada em lote único, com o objetivo de com vistas a evitar problemas relacionados à disponibilização de licenças e a efetiva implantação.

2.2. Poderão ser adquiridos equipamentos, software e serviços conforme quantitativo e especificações mínimas a seguir descritas

	Item	Descrição item	Qtdade	Unidade	Valor unitário máximo
LOTE ÚNICO	1	Roteador remoto SD-WAN com WI-FI (FortiWifi 40F) Código SIASG: 473387	20	Equipamento	R$ 10.213,04
	2	Ponto de acesso WI-FI Código SIASG: 393277	60	Equipamento	R$ 10.876,04
	3	Licenciamento do tipo I (Forticare) para firewall Fortigate 100F, período de 12 (doze) meses Código SIASG: 27456	16	Licença	R$ 6.207,19
	4	Licenciamento do tipo II (UTP) para firewall Fortigate 100F, período de 12 (doze) meses Código SIASG: 27456	16	Licença	R$ 22.083,57
	5	Licenciamento do tipo III (Forticare) para firewall FortiWifi 40F, período de 12 (doze) meses Código SIASG: 27456	760	Licença	R$ 2.623,79
	6	Licenciamento do tipo IV (UTP)	40	Licença	R$ 7.691,40

		para firewall FortiWifi 40F, período de 12 (doze) meses Código SIASG: 27456			
	7	Suporte e garantia FortiNac - 4000 (quatro mil) dispositivos gerenciados - 12 (doze) meses Código SIASG: 27740	4	Serviço	R$ 104.504,20
	8	Solução de Gerenciamento - Fortimanager-vm para 200 (duzentos) dispositivos Código SIASG: 27081	1	Licença	R$ 293.888,76
	9	Solução de logs e relatórios - Fortianalyzer 100Gb/dia Código SIASG: 27081	1	Licença	R$ 334.447,40
	10	Serviço de instalação da Solução de Gerenciamento - Fortimanager-vm Código SIASG: 27359	1	Serviço	R$ 13.932,82
	11	Serviço de instalação da Solução de logs e relatórios – Fortianalyzer Código SIASG: 27359	1	Serviço	R$ 19.005,94

2.3. Os quantitativos acima são suficientes para atender a demanda atual, bem como eventuais expansões futuras na rede da Justiça Eleitoral do Paraná, pelo prazo de vigência da ata de registro de preços, que será de 1 (um) ano, com possibilidade de prorrogação por mais 1 (um) ano, conforme previsão no artigo 84 da Lei de Licitações e Contratos Administrativos (Lei nº 14.133, de 2021).

2.4. Este Tribunal se reserva ao direito de adquirir o quantitativo que julgar necessário, com previsão de compra inicial de:

2.4.1. 5 (cinco) roteadores remotos SD-WAN com WI-FI (item 1);
2.4.2. 10 (dez) pontos de acesso WI-FI (item 2);
2.4.3. 4 (quatro) licenças do tipo I (Forticare) para firewall Fortigate 100F (item 3);
2.4.4. 158 (cento e cinquenta e oito) licenças do tipo III (Forticare) para firewall FortiWifi 40F (item 5);
2.4.5. 1 (um) pacote de suporte e garantia FortiNac - 4000 (quatro mil) dispositivos gerenciados (item 7).

3. DAS ESPECIFICAÇÕES TÉCNICAS E QUANTITATIVOS

3.1. Item 1 – Roteador Remoto SD-WAN com Wi-fi integrado

3.1.1. Características do Equipamento:

3.1.1.1. Deve suportar, no mínimo, 5 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6;
3.1.1.2. Deve suportar, no mínimo, 1 Gbps de throughput IPS;
3.1.1.3. Deve suportar, no mínimo, 4 Gbps de throughput de VPN IPSec;
3.1.1.4. Deve suportar, no mínimo, 300 Mbps de throughput de VPN SSL ou TLS inspection;
3.1.1.5. Deve suportar, no mínimo, 800 Mbps de throughput de Controle de Aplicação;
3.1.1.6. Deve suportar, no mínimo, 500 Mbps de throughput com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: firewall, controle de aplicação, IPS e antimalware;
3.1.1.7. Suporte a, no mínimo, 500.000 conexões simultâneas;
3.1.1.8. Suporte a, no mínimo, 30.000 novas conexões por segundo;
3.1.1.9. Estar licenciado para, ou suportar sem o uso de licença, 180 túneis de VPN IPSEC Site-to-Site simultâneos;
3.1.1.10. Estar licenciado para, ou suportar sem o uso de licença, 220 túneis de clientes VPN IPSEC simultâneos;
3.1.1.11. Estar licenciado para, ou suportar sem o uso de licença adicional, 180 clientes de VPN SSL simultâneos;
3.1.1.12. Permitir gerenciar ao menos 6 Access Points em modo túnel e 12 em modo bridge;
3.1.1.13. Possuir ao menos 4 interfaces 1Gbps;
3.1.1.14. Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 2 sistemas virtuais lógicos (Contextos) por appliance;
3.1.1.15. Suporte a, no mínimo, 2 sistemas virtuais lógicos (Contextos) por appliance;
3.1.1.16. Possuir no máximo 1 RU de altura.
3.1.1.17. Considerando que a presente contratação tem o objetivo de dar continuidade ao projeto de modernização da rede iniciado em 2020, para atendimento aos requisitos de compatibilidade e padronização da solução, os equipamentos a serem fornecidos neste item devem ser do fabricante Fortinet, modelo FortiWiFi 40F, ou superior.

3.1.2. Requisitos Mínimos de Funcionalidade

3.1.2.1. A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;
3.1.2.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
3.1.2.3. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta

especificação;

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

3.1.2.5. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

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

3.1.2.7. Os dispositivos de proteção de rede devem possuir suporte a, no mínimo, 200 VLAN Tags 802.1q;

3.1.2.8. Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP;

3.1.2.9. Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;

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

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

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

3.1.2.13. Os dispositivos de proteção de rede devem suportar sFlow;

3.1.2.14. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet lógicas;

3.1.2.15. Deve suportar NAT dinâmico (Many-to-1);

3.1.2.16. Deve suportar NAT dinâmico (Many-to-Many);

3.1.2.17. Deve suportar NAT estático (1-to-1);

3.1.2.18. Deve suportar NAT estático (Many-to-Many);

3.1.2.19. Deve suportar NAT estático bidirecional 1-to-1;

3.1.2.20. Deve suportar Tradução de porta (PAT);

3.1.2.21. Deve suportar NAT de Origem;

3.1.2.22. Deve suportar NAT de Destino;

3.1.2.23. Deve suportar NAT de Origem e NAT de Destino simultaneamente;

3.1.2.24. Deve poder combinar NAT de origem e NAT de destino na mesma politica

3.1.2.25. Deve implementar Network Prefix Translation (NPTv6) ou NAT66;

3.1.2.26. Deve implementar o protocolo ECMP;

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

3.1.2.28. Deve ser capaz de enviar logs para sistema de monitoramento externo e ser compatível com o software QRadar, utilizado pelo TRE-PR;

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

3.1.2.30. Deve possuir proteção anti-spoofing;

3.1.2.31. Deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2) para IPv4;

3.1.2.32. Suportar OSPF graceful restart;

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

3.1.2.34. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
3.1.2.35. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
3.1.2.36. Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
3.1.2.37. Suporte a configuração de alta disponibilidade Ativo/Passivo ou Ativo/Ativo: Em modo transparente;
3.1.2.38. Suporte a configuração de alta disponibilidade Ativo/Passivo ou Ativo/Ativo: Em layer 3;
3.1.2.39. Suporte a configuração de alta disponibilidade Ativo/Passivo ou Ativo/Ativo: Em layer 3 e com no mínimo 2 equipamentos no cluster;
3.1.2.40. A configuração em alta disponibilidade deve sincronizar: Sessões;
3.1.2.41. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado às políticas de Firewall, NAT, QOS e objetos de rede;
3.1.2.42. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;
3.1.2.43. A configuração em alta disponibilidade deve sincronizar:Tabelas FIB;
3.1.2.44. O modo de Alta-Disponibilidade deve possibilitar monitoração de falha de link;
3.1.2.45. Deve possuir suporte à criação de sistemas virtuais no mesmo appliance;
3.1.2.46. Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo-ativo ou ativo-passivo, permitindo a distribuição de carga entre diferentes contextos;
3.1.2.47. O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado à, exportar configuração dos sistemas virtuais (contextos) por ambas interfaces;
3.1.2.48. Efetuar controle, inspeção e descriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
3.1.2.49. A solução deve identificar potenciais vulnerabilidades e destacar as melhores práticas que poderiam ser usadas para melhorar a segurança e o desempenho geral de uma rede;
3.1.2.50. O console de administração deve suportar pelo menos inglês;
3.1.2.51. O console deve suportar o gerenciamento de pontos de acesso wireless;

3.1.3. Controle por Política de Firewall:

3.1.3.1. Deverá suportar controles por zona de segurança;
3.1.3.2. Efetuar controles de políticas por porta e protocolo;
3.1.3.3. Efetuar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
3.1.3.4. Deve efetuar controle de políticas por usuários, grupos de

usuários, IPs, redes e zonas de segurança;

3.1.3.5. Deve suportar a automação de situações como detecção de equipamentos comprometidos, status do sistema, alterações de configuração, eventos específicos e aplicar uma ação que pode ser notificação, bloqueio de um computador, execução de scripts ou funções em nuvem pública;

3.1.3.6. Deve suportar o padrão de indústria 'syslog' protocol para armazenamento usando o formato Common Event Format (CEF);

3.1.3.7. Deve suportar objetos de endereço IPv4 e IPv6, consolidados na mesma regra/política de firewall

3.1.3.8. Deve possuir base com objetos de endereço IP, de serviços da internet como Google e Office 365, atualizados dinamicamente pela solução;

3.1.3.9. A solução deve oferecer suporte à integração nativa com a solução de sandbox, proteção de email, cache e firewall de aplicativos da Web.

3.1.4. Controle de Aplicações:

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

3.1.4.2. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

3.1.4.3. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

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

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

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

3.1.4.7. Atualizar a base de assinaturas de aplicações automaticamente;

3.1.4.8. Deve estar apto a limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;

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

3.1.4.10. O fabricante deve permitir a solicitação de inclusão de

aplicações na base de assinaturas de aplicações;

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

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

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

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

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

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

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

3.1.4.18. Deve ser possível configurar Application Override permitindo selecionar aplicações individualmente.

3.1.5. Prevenção de Ameaças:

3.1.5.1. Para este item a solução deve suportar o licenciamento futuro com suporte a performance do item 3.1.6;

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

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

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

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

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

3.1.5.7. Deve permitir o bloqueio de vulnerabilidades;

3.1.5.8. Deve incluir proteção contra ataques de negação de serviços;

3.1.5.9. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise de decodificação de protocolo;

3.1.5.10. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise para detecção de anomalias de protocolo;

3.1.5.11. Deverá possuir o seguinte mecanismos de inspeção de IPS: IP Defragmentation;

3.1.5.12. Deverá possuir o seguinte mecanismos de inspeção de IPS:

Remontagem de pacotes de TCP;

3.1.5.13. Deverá possuir o seguinte mecanismos de inspeção de IPS: Bloqueio de pacotes malformados;

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

3.1.5.15. Detectar e bloquear a origem de port scans;

3.1.5.16. Bloquear ataques efetuados por worms conhecidos;

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

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

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

3.1.5.20. Identificar e bloquear comunicação com botnets;

3.1.5.21. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

3.1.5.22. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;

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

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

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

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

3.1.5.27. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;

3.1.5.28. Suportar e estar licenciado com proteção contra ataques de dia zero por meio de integração com solução de Sandbox em nuvem, do mesmo fabricante;

3.1.5.29. Mesmo sem o licenciamento deste recurso de Proteção de Ameaças, deve ser possível criar assinaturas de modo manual para tratar a inspeção até a camada 7 do modelo OSI (Aplicação).

3.1.6. Filtro de URL:

3.1.6.1. Para este item a solução deve suportar o licenciamento futuro;

3.1.6.2. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

3.1.6.3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local, em modo de proxy transparente e explícito;

3.1.6.4. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
3.1.6.5. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
3.1.6.6. Possuir pelo menos 60 categorias de URLs;
3.1.6.7. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
3.1.6.8. Permitir a customização de página de bloqueio;
3.1.6.9. Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);
3.1.6.10. Além do Explicit Web Proxy, suportar proxy Web transparente;
3.1.6.11. Mesmo sem o licenciamento deste recurso, deve ser possível criar regras de filtro URL de modo manual com suporte a expressões regulares.

3.1.7. Identificação de Usuários:

3.1.7.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;
3.1.7.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
3.1.7.3. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle / políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à, utilização de sistemas virtuais, segmentos de rede, etc;
3.1.7.4. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle / políticas baseadas em usuários e grupos de usuários;
3.1.7.5. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle / políticas baseadas em Usuários e Grupos de usuários;
3.1.7.6. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
3.1.7.7. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
3.1.7.8. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
3.1.7.9. Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e

gerenciamento da solução;

3.1.7.10. Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator.

3.1.8. QoS e Traffic Shaping:

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

3.1.8.2. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;

3.1.8.3. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;

3.1.8.4. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;

3.1.8.5. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

3.1.8.6. Suportar a criação de políticas de QoS e Traffic Shaping por porta;

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

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

3.1.8.9. O QoS deve possibilitar a definição de fila de prioridade;

3.1.8.10. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

3.1.8.11. Suportar modificação de valores DSCP para o Diffserv;

3.1.8.12. Suportar priorização de tráfego usando informação de Type of Service;

3.1.8.13. Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes.

3.1.9. Filtro de Dados:

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

3.1.9.2. Os arquivos devem ser identificados por extensão e tipo;

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

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

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

3.1.9.6. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de

dados via expressão regular.

3.1.10. Geolocalização:

3.1.10.1. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País / Países sejam bloqueados;
3.1.10.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
3.1.10.3. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

3.1.11. VPN:

3.1.11.1. Suportar VPN Site-to-Site e Client-To-Site;
3.1.11.2. Suportar IPSec VPN;
3.1.11.3. Suportar SSL VPN;
3.1.11.4. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;
3.1.11.5. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
3.1.11.6. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
3.1.11.7. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
3.1.11.8. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
3.1.11.9. Suportar VPN em em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
3.1.11.10. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;
3.1.11.11. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
3.1.11.12. Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, Antispyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
3.1.11.13. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
3.1.11.14. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
3.1.11.15. Deverá manter uma conexão segura com o portal durante a sessão;
3.1.11.16. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);
3.1.11.17. Deve suportar agregação de túneis IPSec
3.1.11.18. Deve suportar algoritmo de balanceamento do tipo WRR (Weighted Round Robin) em agregação de túneis IPSec
3.1.11.19. A VPN IPSec deve suportar Forward Error Correction (FEC)
3.1.11.20. Deve suportar TLS 1.2 em VPN SSL.

3.1.12. Wireless Controller:

3.1.12.1. Deverá administrar e controlar de maneira centralizada os pontos de acesso wireless do mesmo fabricante da solução ofertada;

3.1.12.2. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;

3.1.12.3. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac e que transmitam tráfego IPv4 e IPv6 através do controlador;

3.1.12.4. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor;

3.1.12.5. O controlador wireless deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;

3.1.12.6. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;

3.1.12.7. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;

3.1.12.8. 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 o controlador wireless. Neste modo todos os pacotes devem ser tunelados até o controlador wireless;

3.1.12.9. Quando tunelado, o tráfego deve ser criptografado através de DTLS ou IPSEC;

3.1.12.10. Deve permitir o gerenciamento de pontos de acesso conectados remotamente através de links WAN. Neste cenário o encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma distribuída (local switching), ou seja, o tráfego deve ser comutado localmente na interface LAN do ponto de acesso e não necessitará de tunelamento até o controlador wireless;

3.1.12.11. Quando o encaminhamento do tráfego for distribuído (local switching) e a autenticação via PSK, caso haja falha na comunicação entre os pontos de acesso e o controlador wireless, os usuários associados devem permanecer associados aos pontos de acesso e ao mesmo SSID. Deve ser possível ainda permitir a conexão de novos usuários à rede wireless;

3.1.12.12. A solução deve permitir definir quais redes serão tuneladas até a controladora e quais redes serão comutadas diretamente pela interface do ponto de acesso;

3.1.12.13. A solução deve suportar recurso de Split-Tunneling de forma que seja possível definir, através das sub redes de destino, quais pacotes serão tunelados até a controladora e quais serão comutados localmente na interface do ponto de acesso;

3.1.12.14. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;

3.1.12.15. 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 dBm;

3.1.12.16. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;

3.1.12.17. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;

3.1.12.18. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;

3.1.12.19. A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de Off-channel/Background scanning. Quando realizada através de Off-channel/Background scanning, a solução deve ser capaz de identificar a utilização do ponto de acesso para, caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;

3.1.12.20. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless;

3.1.12.21. A solução deve permitir a adição de controlador redundante operando em N+1. Neste modo, o controlador redundante deve monitorar a disponibilidade e sincronizar as configurações do principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;

3.1.12.22. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas sub redes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;

3.1.12.23. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;

3.1.12.24. A solução deve garantir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;

3.1.12.25. A solução deve implementar o padrão IEEE 802.11r para

acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;

3.1.12.26. A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;

3.1.12.27. A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;

3.1.12.28. A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;

3.1.12.29. A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;

3.1.12.30. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;

3.1.12.31. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;

3.1.12.32. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;

3.1.12.33. A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados para as frequências de 2.4 e 5GHz e padrões 802.11a/b/g/n/ac;

3.1.12.34. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;

3.1.12.35. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;

3.1.12.36. A solução deve permitir a configuração do valor de Short Guard Interval para 802.11n e 802.11ac em 5GHz;

3.1.12.37. A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime alocando porcentagens a serem utilizadas nos SSIDs;

3.1.12.38. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados:

3.1.12.39. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding);

3.1.12.40. Os seguintes ataques de negação de serviço:

3.1.12.40.1. Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication;
3.1.12.40.2. ASLEAP;
3.1.12.40.3. Null Probe Response / Null SSID Probe Response;
3.1.12.40.4. Long Duration;
3.1.12.40.5. Ataques contra Wireless Bridges;
3.1.12.40.6. Weak WEP;
3.1.12.40.7. Invalid MAC OUI.

3.1.12.41. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication;
3.1.12.42. A solução deve implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede wireless;
3.1.12.43. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes wireless;
3.1.12.44. Permitir configurar o bloqueio na comunicação entre os clientes wireless conectados a um determinado SSID;
3.1.12.45. Deve implementar autenticação administrativa através do protocolo RADIUS;
3.1.12.46. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
3.1.12.47. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;
3.1.12.48. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;
3.1.12.49. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;
3.1.12.50. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
3.1.12.51. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;
3.1.12.52. A solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
3.1.12.53. A solução deve implementar recurso para autenticação dos usuários através da página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede;
3.1.12.54. A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;
3.1.12.55. A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;
3.1.12.56. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;
3.1.12.57. A solução deve permitir que a página de autenticação seja

hospedada em servidor externo;

3.1.12.58. A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;

3.1.12.59. A solução deve garantir que usuários se autentiquem em captive portal que faça uso de endereço IPv6;

3.1.12.60. A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;

3.1.12.61. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;

3.1.12.62. A solução deve implementar recurso de DHCP Server (IPv4 e IPv6) para facilitar a configuração de redes visitantes;

3.1.12.63. A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;

3.1.12.64. A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;

3.1.12.65. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;

3.1.12.66. A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;

3.1.12.67. A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;

3.1.12.68. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;

3.1.12.69. A solução deve permitir ser gerenciada através do protocolo SNMP (v1, v2c e v3), além de emitir notificações através da geração de traps;

3.1.12.70. A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP;

3.1.12.71. A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB);

3.1.12.72. A solução deve permitir a captura de pacotes na rede wireless e exportá-los em arquivos no formato .pcap;

3.1.12.73. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;

3.1.12.74. A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;

3.1.12.75. A solução deve implementar o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;

3.1.12.76. A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;

3.1.12.77. A solução deve permitir a identificação do firmware utilizado

por cada ponto de acesso gerenciado e permitir a atualização individualizada através da interface gráfica;

3.1.12.78. A solução deve possuir ferramentas de diagnósticos e debug;

3.1.12.79. A solução deve suportar comunicação com elementos externos através de APIs;

3.1.12.80. A solução deverá ser compatível e gerenciar os pontos de acesso deste processo;

3.1.13. SD-WAN:

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

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

3.1.13.1.3. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links.

3.1.13.1.4. Deve implementar balanceamento de link por custo configurado do link.

3.1.13.1.5. Deve suportar o balanceamento de, no mínimo, 5 links;

3.1.13.1.6. Deve suportar o balanceamento de links de interfaces físicas, sub-interfaces lógicas de VLAN e túneis IPSec

3.1.13.1.7. Deve suportar o balanceamento de links LTE (4G) sem restrições de uso, podendo ser usado em conjunto com outros links e não ser somente o backup para todos os outros links.

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

3.1.13.1.9. Deve gerar log de eventos que registrem alterações no estado dos links do SDWAN, monitorados pela checagem de saúde

3.1.13.1.10. Deve suportar Zero-Touch Provisioning

3.1.13.1.11. Possuir checagem do estado de saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Perda de Pacotes

3.1.13.1.12. Deve ser possível configurar a porcentagem de perda de pacotes e o tempo de latência e jitter, na medição de estado de link. Estes valores serão utilizados pela solução para decidir qual link será utilizado

3.1.13.1.13. A solução deve permitir modificar o intervalo de tempo de checagem, em segundos, para cada um dos links.

3.1.13.1.14. A checagem de estado de saúde deve suportar teste com Ping, HTTP e DNS

3.1.13.1.15. Suportar UDP Hole Punching em arquitetura ADVPN

3.1.13.1.16. A checagem de estado de saúde deve suportar a marcação de pacotes com DSCP, para avaliação mais precisa de links que possuem QoE configurado

3.1.13.1.17. As regras de escolha do link SD-WAN devem suportar o reconhecimento de aplicações, grupos de usuários, endereço IP de destino e Protocolo.

3.1.13.1.18. Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SD-WAN

3.1.13.1.19. Deve suportar envio de BGP route-map para BGP

neighbors, caso a qualidade mínima de um link não seja detectada pela checagem de saúde do link.

3.1.14. Access Point:

3.1.14.1. O equipamento deve possuir uma antena integrada para acesso wi-fi de clientes. Se o equipamento ofertado não possuir esta antena, o atendimento a este item poderá ser composto com a entrega de um equipamento adicional para casa roteador remoto adquirido, conforme especificações do item 3 deste lote;
3.1.14.2. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;
3.1.14.3. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac em Wave2;
3.1.14.4. Deve suportar operação nas faixas de frequência de 2.4GHz e 5GHz;
3.1.14.5. Deve suportar MU-MIMO 3x3;
3.1.14.6. Deve possuir antenas externas no equipamento com ganho mínimo de 5dBi em 2.4GHz e 3.5dBi em 5GHz;
3.1.14.7. Deve suportar uma potência de transmissão de no mínimo 20 dBm;
3.1.14.8. Deve suportar velocidades mínimas de 1300 Mbps em 5GHz e 450 Mbps em 2.4GHz;

3.2. <u>Item 2 – Ponto de Acesso Wi-fi</u>

3.2.1. Deve ser do tipo Indoor;
3.2.2. Deverá possuir três rádios, sendo eles:
3.2.2.1. O primeiro rádio deve suportar Taxa de transmissão de no mínimo 574 Mbps e ser configurável para operar em 2.4GHz;
3.2.2.2. O segundo rádio deve suportar Taxa de transmissão de no mínimo 1200 Mbps e operar em 5GHz;
3.2.2.3. O terceiro rádio deverá operar em modo dedicado a escaneamento de radiofrequência 24/7 em 2.4GHz e 5GHz, provendo informações de WIDS, Rogue Scanning, etc;
3.2.3. Suportar no mínimo 512 (quinhentos e doze) usuários associados nos rádios 1 e 2;
3.2.4. Deverá possuir também um Rádio do Tipo BLE, além dos rádios explicitados acima;
3.2.5. Implementar as tecnologias 802.11 a/b/g/n/ac-W2/ax;
3.2.6. Implementar SU-MIMO 2x2;
3.2.7. Implementar 802.11ac Wave2 e 802.11ax (Wi-Fi6);
3.2.8. Implementar MU-MIMO;
3.2.9. Deve permitir que o terceiro rádio seja utilizado como analisador de espectro;
3.2.10. Implementar 802.11ac VHT 20/40/80 MHz;
3.2.11. Ter potência máxima de ao menos 23 dBm considerando 2.4GHz;
3.2.12. Sensibilidade RX de ao menos -86 dBm considerando tráfego em VHT40 para MCS 0;
3.2.13. Ter ao menos 3 antenas internas;
3.2.14. O ganho das antenas internas em 2.4GHz deve ser ao menos 4 dBi;
3.2.15. O ganho das antenas internas em 5GHz deve ser ao menos 5 dBi;
3.2.16. Ter 1 antena interna do tipo BLE;

3.2.17. A antena do tipo BLE deve possuir potência de ao menos 5 dBm;
3.2.18. Deve possuir 2 interfaces de rede operando em velocidades de 10/100/1000Mbps, sendo 1 com capacidade de alimentação do equipamento via PoE (PoE 802.3af);
3.2.19. Possuir interface de console;
3.2.20. Possuir local para conexão de trava Kensington;
3.2.21. Deve suportar temperatura de operação até 40 º C;
3.2.22. Implementar Transmit Beamforming (TxBF);
3.2.23. Possuir certificado WPA3;
3.2.24. Deve permitir sua implementação em modo Bridge, Mesh e Tunel;
3.2.25. O Fabricante da solução deve possuir ferramenta própria de controle de acesso à rede (NAC), permitindo que posteriormente sejam implementados serviços como Device Profiling, descoberta de rede, Políticas de Controle de Acesso, Micro-Segmentação, Endpoint Compliance e autenticação avançada com Agentes.
3.2.26. Considerando que a presente contratação tem o objetivo de dar continuidade ao projeto de modernização da rede iniciado em 2020, para atendimento aos requisitos de compatibilidade e padronização da solução, os equipamentos a serem fornecidos neste item devem ser do fabricante Fortinet, modelo FortiAP 231F, ou superior.

3.3. Requisitos Mínimos de Funcionalidade - Características Gerais

3.3.1. Ponto de acesso (AP) que permita acesso dos dispositivos à rede através da wireless (sem fio) e que permita que as suas configurações sejam centralizadas em controlador wireless;
3.3.2. Deve suportar modo de operação centralizado, ou seja, sua operação depende do controlador wireless que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência;
3.3.3. Deve acompanhar licença que permita que sejam habilitadas todas as suas funcionalidades;
3.3.4. Deve identificar automaticamente o controlador wireless ao qual se conectará;
3.3.5. Deve permitir ser gerenciado remotamente através de links WAN;
3.3.6. Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;
3.3.7. 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 devem ser tunelados até o controlador wireless;
3.3.8. Quando tunelado, o tráfego deve ser criptografado através de DTLS ou IPSEC;
3.3.9. Deve permitir o gerenciamento de pontos de acesso conectados remotamente através de links WAN. Neste cenário o encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma distribuída (local switching), ou seja, o tráfego deve ser comutado localmente na interface LAN do ponto de acesso e não necessitará de tunelamento até o controlador wireless;
3.3.10. Quando o encaminhamento do tráfego for distribuído (local switching) e a autenticação via PSK, caso haja falha na comunicação entre os pontos de acesso e o controlador wireless, os usuários associados devem permanecer associados aos pontos de acesso e ao mesmo

SSID. Deve ser possível ainda permitir a conexão de novos usuários à rede wireless;

3.3.11. Em conjunto com o controlador wireless, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados;

3.3.12. Possuir funcionalidade de ajuste de potência automática de forma a estender cobertura no caso de falha de APs vizinhos gerenciados pela mesma controladora;

3.3.13. Deve suportar mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs;

3.3.14. Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS);

3.3.15. Em conjunto com o controlador wireless, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede;

3.3.16. Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);

3.3.17. Em conjunto com o controlador wireless, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;

3.3.18. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;

3.3.19. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;

3.3.20. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;

3.3.21. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;

3.3.22. Deve implementar o padrão IEEE 802.11e;

3.3.23. Deve implementar o padrão IEEE 802.11h;

3.3.24. Implementar agregação de pacotes A-MPDU e A-MSDU no Access Point;

3.3.25. Implementar LPDC - Low Density Parity Check no Access Point;

3.3.26. Implementar (MLD) - Maximum Likelihood Demodulation no Access Point;

3.3.27. Implementar Maximum Ratio Combining (MRC) no Access Point;

3.3.28. Deve possuir indicadores luminosos (LED) para indicação de status;

3.3.29. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at;

3.3.30. O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores wireless deste processo;

3.3.31. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;

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

3.3.33. Deve ser fornecido com garantia do tipo NBD para no mínimo 24 meses

3.3.34. Deve ser fornecido com kit de montagem para teto, permitindo que o Ponto de Acesso seja instalado em superfícies planas, como tetos;

3.4. Item 3 - Licenciamento do tipo I (Forticare) para firewall Fortigate 100F, período de 12 meses

3.4.1. Fornecimento de licenciamento do tipo Forticare, pelo período de 12 meses, para os equipamentos Fortigate 100F, do fabricante Fortinet em uso no TRE-PR;
- 3.4.1.1. Part number: FC-10-F100F-247-02-12

3.4.2. O licenciamento a ser fornecido deve permitir:
- 3.4.2.1. Manutenção de Hardware: Reparo e substituição de equipamentos em caso de defeitos;
- 3.4.2.2. Atualização de Software: Disponibilização de novas versões de software (firmware), funcionalidades, correções e atualizações de versões;
- 3.4.2.3. Suporte Técnico Especializado provido pela fabricante (ou integrador) para diagnóstico e solução de problemas;

3.5. Item 4 - Licenciamento do tipo II (UTP) para firewall Fortigate 100F, período de 12 meses

3.5.1. Fornecimento de licenciamento na modalidade na modalidade Unified Threat Protection (UTP), pelo período de 12 meses, para os equipamentos Fortigate 100F, do fabricante Fortinet em uso no TRE-PR;
- 3.5.1.1. Part number: FC-10-F100F-950-02-12

3.5.2. O licenciamento a ser fornecido deve permitir:
- 3.5.2.1. Manutenção de Hardware: Reparo e substituição de equipamentos em caso de defeitos;
- 3.5.2.2. Atualização de Software: Disponibilização de novas versões de software (firmware), funcionalidades, correções e atualizações de versões;
- 3.5.2.3. Suporte Técnico Especializado provido pela fabricante (ou integrador) para diagnóstico e solução de problemas;

3.5.3. O licenciamento aqui proposto deve permitir, pelo menos, a utilização das seguintes funcionalidades, conforme detalhado no item 1 deste mesmo documento:

- 3.5.3.1. Controle de Aplicações;
- 3.5.3.2. Prevenção de Ameaças;
- 3.5.3.3. Filtro de URL;
- 3.5.3.4. Filtro de Dados;
- 3.5.3.5. Geolocalização;

3.6. Item 5 - Licenciamento do tipo III (Forticare) para firewall FortWifi 40F, período de 12 meses

3.6.1. Fornecimento de licenciamento do tipo Forticare, pelo período de 12 meses, para os equipamentos Fortigate 40F, do fabricante Fortinet em uso no TRE-PR;
- 3.6.1.1. Part number:FC-10-W040F-247-02-12

3.6.2. O licenciamento a ser fornecido deve permitir:

3.6.2.1. Manutenção de Hardware: Reparo e substituição de equipamentos em caso de defeitos;
3.6.2.2. Atualização de Software: Disponibilização de novas versões de software (firmware), funcionalidades, correções e atualizações de versões;
3.6.2.3. Suporte Técnico Especializado provido pela fabricante (ou integrador) para diagnóstico e solução de problemas;

3.7. <u>Item 6 - Licenciamento do tipo IV (UTP) para firewall FortiWifi 40F, período de 12 meses</u>

3.7.1. Fornecimento de licenciamento na modalidade na modalidade Unified Threat Protection (UTP), pelo período de 12 meses, para os equipamentos Fortigate 40F, do fabricante Fortinet em uso no TRE-PR;
3.7.1.1. Part number: FC-10-W040F-950-02-12
3.7.2. O licenciamento a ser fornecido deve permitir:
3.7.2.1. Manutenção de Hardware: Reparo e substituição de equipamentos em caso de defeitos;
3.7.2.2. Atualização de Software: Disponibilização de novas versões de software (firmware), funcionalidades, correções e atualizações de versões;
3.7.2.3. Suporte Técnico Especializado provido pela fabricante (ou integrador) para diagnóstico e solução de problemas;
3.7.3. O licenciamento aqui proposto deve permitir, pelo menos, a utilização das seguintes funcionalidades, conforme detalhado no item 1 deste mesmo documento:

3.7.3.1. Controle de Aplicações;
3.7.3.2. Prevenção de Ameaças;
3.7.3.3. Filtro de URL;
3.7.3.4. Filtro de Dados;
3.7.3.5. Geolocalização;

3.8. <u>Item 7 - Suporte e garantia FortiNac- 4000 dispositivos gerenciados - 12 meses</u>

3.8.1. Fornecimento de licenciamento do tipo Forticare, pelo período de 12 meses, para o software FortiNac, do fabricante Fortinet, instalado e em uso no TRE-PR;
3.8.1.1. Part number: 40x FC2-10-FNAC0-240-02-12

3.8.2. O licenciamento a ser fornecido deve permitir:

3.8.2.1. Atualização de Software: Disponibilização de novas versões de software (firmware), funcionalidades, correções e atualizações de versões;
3.8.2.2. Suporte Técnico Especializado provido pela fabricante (ou integrador) para diagnóstico e solução de problemas;

3.9. <u>Item 8 - Solução de Gerenciamento - Fortimanager-vm para 200 dispositivos</u>

3.9.1. Fornecimento do software FortiManager-VM

3.9.1.1. Part Numbers: : 2 x FMG-VM-100-UG e 1 x FC3-10-M3004-248-02-24

3.9.2. A solução deve ser capaz de:

3.9.2.1. Efetuar o gerenciamento centralizado orientado por automação de até 200 dispositivos do fabricante Fortinet instalados nas dependências do TRE-PR;

3.9.2.2. Permitir a administração total e a visibilidade dos dispositivos de rede;

3.9.2.3. Integrar-se com a arquitetura de segurança permitindo otimizar as atividades de monitoramento e gerenciamento do ambiente;

3.9.2.4. Possuir, no mínimo, suporte para instalação em hypervisor VMware ESX/ESXi 6.5/6.7/7.0;

3.9.2.5. Permitir a atualização de software/firmware pelo período 24 meses;

3.10. Item 9 - Solução de logs e relatórios - Fortianalyzer 100Gb/dia

3.10.1. Fornecimento do software Fortinet FortiAnalyzer com Part Numbers: 1 x FAZ-VM-GB100 e 1 x FC4-10-LV0VM-248-02-24

3.10.2. A solução a ser fornecida deve ser capaz de:

3.10.2.1. FortiAnalyzer Virtual Appliance (FAZ-VM-BASE e FAZ-VM-GB25):

3.10.2.2. Monitorar o tráfego e atividade da rede de dados do TRE-PR;

3.10.2.3. Apresentar histórico e fornecer relatórios das atividades realizadas na

3.10.2.4. administração e operação da solução, bem como de todo o tráfego controlado e

3.10.2.5. monitorado pela mesma.

3.10.2.6. Possuir capacidade de até 100GB diária de logs;

3.10.2.7. Possuir capacidade de armazenamento mínimo de 10 TB;

3.10.2.8. Possuir, no mínimo, suporte para instalação em hypervisor VMware ESX/ESXi 6.5/6.7/7.0;

3.10.2.9. Permitir a atualização de software/firmware pelo período 24 meses;

3.11. Item 10 - Serviço de instalação da Solução de Gerenciamento - Fortimanager-vm

3.11.1. A realização dos serviços deve ser planejada de acordo com disponibilidade de ambas as partes. O planejamento anterior ao serviço deverá ser realizado de forma on-site nas dependências da CONTRATANTE;

3.11.2. 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;

3.11.3. 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;

3.11.4. 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.

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

3.11.6. Os serviços, que terão duração mínima de 24 horas úteis, 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;

3.11.7. 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.

3.11.7.1. Este relatório deve ser enviado com todas as informações em até 15 (quinze)dias após a finalização dos serviços;

3.11.8. Todos os equipamentos atualmente em uso na contratada devem ser incluídos na solução de gerenciamento implantada;

3.11.9. Nos valores cotados devem estar inclusas todas as despesas com deslocamento, alimentação e estadia para realização dos serviços (onsite) nos locais de presença da CONTRATANTE.

3.11.10. Os funcionários da CONTRATADA deverão possuir todo o ferramental necessário ao exercício das suas atividades;

3.11.11. A CONTRATADA deverá garantir a confidencialidade das informações, dados e senhas compartilhadas da CONTRATANTE, conforme previsto neste edital;

3.11.12. As atividades deverão ser realizadas dentro do horário normal de funcionamento do TRE-PR, isto é, entre 12h e 19h;

A implantação não deverá se limitar somente às configurações aqui destacadas. Quaisquer novas funcionalidades suportadas poderão fazer parte do escopo do projeto. Estas informações serão documentadas no termo de abertura do projeto a ser documentado pela CONTRATADA após alinhamento do escopo de trabalho entre CONTRATADA e CONTRATANTE;

3.11.13. 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).

3.12. Item 11 - Serviço de instalação da Solução de logs e relatórios - Fortianalyzer

3.12.1. A realização dos serviços deve ser planejada de acordo com disponibilidade de ambas as partes. O planejamento anterior ao serviço deverá ser realizado de forma on-site nas dependências da CONTRATANTE;

3.12.2. 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;

3.12.3. 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;

3.12.4. 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.

3.12.5. Ao final da instalação, deverá ser realizado o repasse de configurações hands-on, de forma remota ou presencial,

apresentando as configurações realizadas nos equipamentos pelo prazo mínimo de 8 (oito) horas corridas;

3.12.6. Os serviços, que terão duração mínima de 24 horas úteis, 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;

3.12.7. 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.

3.12.7.1. Este relatório deve ser enviado com todas as informações em até 15 (quinze)dias após a finalização dos serviços;

3.12.8. Todos os equipamentos atualmente em uso na contratada devem ser incluídos na solução de logs e relatórios a ser implantada;

3.12.9. Nos valores cotados devem estar inclusas todas as despesas com deslocamento, alimentação e estadia para realização dos serviços (onsite) nos locais de presença da CONTRATANTE.

3.12.10. Os funcionários da CONTRATADA deverão possuir todo o ferramental necessário ao exercício das suas atividades;

3.12.11. A CONTRATADA deverá garantir a confidencialidade das informações, dados e senhas compartilhadas da CONTRATANTE, conforme previsto nesteTermo de Referência;

3.12.12. As atividades deverão ser realizadas dentro do horário normal de funcionamento do TRE-PR, isto é, entre 12h e 19h;

3.12.13. A implantação não deverá se limitar somente às configurações aqui destacadas. Quaisquer novas funcionalidades suportadas poderão fazer parte do escopo do projeto. Estas informações serão documentadas no termo de abertura do projeto a ser documentado pela CONTRATADA após alinhamento do escopo de trabalho entre CONTRATADA e CONTRATANTE;

3.12.14. 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).

4. DAS ESPECIFICAÇÕES TÉCNICAS E QUANTITATIVOS

4.1. DA ENTREGA DO OBJETO

4.1.1. Todos os equipamentos entregues devem ser de uma única marca e modelo.

4.1.1.1. A contratada deverá apresentar os equipamentos acondicionados conforme padrão do fabricante. A embalagem deve garantir a proteção do equipamento durante o transporte e estocagem, bem como conter a identificação do produto e demais informações que facilitem a verificação e manuseio dos mesmos.

4.1.2. Deverá ser fornecida documentação completa e atualizada (manuais, termos de garantia, etc.), no idioma português, e em quantidade necessária à instalação e à operação dos equipamentos;

4.1.3. A Contratada deverá fixar nos equipamentos chapa/etiqueta com número de controle patrimonial, a ser fornecida pelo Tribunal Regional Eleitoral do Paraná juntamente com as instruções para fixação das mesmas.

4.1.4. Todas as licenças mencionadas na presente contratação devem ser entregues no mínimo em formato digital, com a possibilidade de constante comprovação e verificação de todas as características e informações. Caso seja necessário encaminhamento de informações ou artefatos referentes ao licenciamento, poderá ser utilizado o e-mail da Seção de Rede: rede@tre-pr.jus.br, ou qualquer outro endereço acordado para a comunicação entre as partes.

4.1.5. **DO LOCAL DE ENTREGA E PRESTAÇÃO DOS SERVIÇOS:** Os equipamentos deverão ser entregues e os serviços prestados na Seção de Rede deste Tribunal, mediante agendamento pelo telefone 41 - 3330-8628.

4.1.5.1. A entrega dos equipamentos e a prestação de serviços deverão ser feitos em dias úteis – segunda a sexta-feira – no horário compreendido entre as 13 e as 19 horas, podendo também ocorrer, caso o TRE julgue necessário, em sábados, domingos e feriados.

4.1.6. DO PRAZO DE ENTREGA:

4.1.6.1. **Para os itens 01 e 02**: prazo máximo de 60 (sessenta) dias corridos contados da assinatura do contrato, estando incluso no valor contratado quaisquer despesas com frete e demais impostos inerentes à contratação;

4.1.6.2. **Para os itens 03 a 09:** o fornecimento das licenças e o início da prestação de suporte ou garantia deverão ser efetivados no prazo máximo de 15 (quinze) dias corridos contados da assinatura do contrato;

4.1.6.3. **Para os itens 10 e 11**: prazo de 40 dias corridos contados da assinatura do contrato;

4.1.6.4. Não serão aceitas entregas no período de recesso deste TRE, ou seja, entre 20 de dezembro e 6 de janeiro.

4.2. DO RECEBIMENTO

4.2.1. DO RECEBIMENTO PROVISÓRIO

4.2.1.1. O recebimento provisório, para qualquer dos itens em comento na presente contratação, será realizado por servidor lotado na Seção de Rede, no prazo máximo de 05 (cinco) dias corridos contados a partir da entrega.

4.2.2. DO RECEBIMENTO TÉCNICO E DEFINITIVO

4.2.2.1. Comissão Técnica com no mínimo 03 (três) servidores a ser instituída pela Secretaria de Tecnologia da Informação realizará, no prazo máximo de 03 (três) dias úteis a partir do recebimento provisório, uma inspeção técnica dos equipamentos adquiridos para verificação da sua integridade física e cumprimento das especificações exigidas no edital e seus anexos;

4.2.2.2. Para a inspeção técnica, será utilizada a documentação entregue pelo fornecedor e/ou fabricante do equipamento contendo as especificações detalhadas dos itens licitados, constantes da proposta detalhada (anexo III);

4.2.2.3. A inspeção técnica poderá ser realizada por amostragem, a critério da Administração. O equipamento que, a qualquer tempo durante a vigência do contrato, apresentar irregularidades ou estiver em desacordo com aquele aprovado durante a análise da amostra deverá ser substituído no prazo de até 05 (cinco) dias, contados do comunicado enviado pelo TRE-PR.

4.2.2.4. Os equipamentos deverão ser entregues em perfeito estado de funcionamento, sem marcas, amassados, arranhões e/ou outros problemas físicos;

4.2.2.5. O equipamento testado deverá possuir todos os componentes e as mesmas características do equipamento ofertado no edital, sendo aceitos componentes e especificações superiores;

4.2.2.6. Após a inspeção técnica nos equipamentos e verificando que estes estão em perfeitas condições de funcionamento, Comissão Técnica a ser instituída pela Secretaria de Tecnologia da Informação emitirá(ão) o Atestado de Aceite Técnico e encaminhará ao gestor da contratação para emissão do ateste definitivo, no prazo máximo informado no item 4.2.2.1.

4.2.2.7. A Coordenadoria de Infraestrutura receberá e encaminhará a nota fiscal e atestado do bem no prazo máximo de 02 (dois) dias úteis a partir da emissão do aceite técnico.

4.2.2.8. Recebido o objeto, mas constatado qualquer defeito/irregularidade, a Contratada deverá providenciar a substituição no prazo de até 05 (cinco) dias, contados do comunicado do TRE/PR, sem quaisquer ônus.

5. DAS OBRIGAÇÕES DA CONTRATADA

5.1. DA SUSTENTABILIDADE

5.1.1. Os equipamentos a serem entregues devem estar em conformidade com as diretrizes RoHS;

5.1.2. As unidades do equipamento deverão ser entregues devidamente acondicionadas em embalagens individuais adequadas, que utilizem, preferencialmente, materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e a armazenagem;

5.1.3. A contratada para o fornecimento dos equipamentos, na qualidade de fabricante, importador, distribuidor ou comerciante, poderá ser solicitada a providenciar o recolhimento e o adequado descarte do lixo tecnológico originário desta aquisição de equipamentos, entendido como aqueles produtos ou componentes eletrônicos em desuso e sujeitos a disposição final, para fins de sua destinação final ambientalmente adequada, conforme a lei 12.305/2010, artigo 33 caput, inciso VI e seus parágrafos;

5.2. DOS REQUISITOS DE SUPORTE E GARANTIA DOS EQUIPAMENTOS E SOFTWARE (Itens 1, 2, 8, E 9)

5.2.1. A garantia de funcionamento para os equipamentos entregues será pelo período de 24 (vinte e quatro) meses contados a partir do Recebimento Definitivo do componente, sem prejuízo de qualquer política de garantia adicional oferecida pelo fabricante.

5.2.2. Caso haja garantia adicional oferecida pelo fabricante, a Contratada deverá descrever os seus termos na Proposta Detalhada (anexo III).

5.2.3. A garantia deve incluir todo e qualquer defeito decorrente de projeto, fabricação, construção, montagem, acondicionamento, transporte ou desgaste prematuro, com a substituição de peças, componentes, ajustes, reparos e correções necessárias, às expensas da contratada;

5.2.4. O fornecedor não poderá, em hipótese alguma, negar-se a registrar chamadas relacionadas ao equipamento adquirido, ainda que se conclua, ao final, que a solução do incidente não seja de responsabilidade do fornecedor/fabricante;

5.2.5. O prazo máximo para o primeiro atendimento dos chamados é de 02 (dois) dias úteis, contados a partir da abertura do chamado;

5.2.6. O prazo máximo para a solução do problema é de 3 (três) dias úteis contados a partir do primeiro atendimento, mesmo incluindo a troca de peças e/ou componentes mecânicos ou eletrônicos;

5.2.7. Em caso de substituição de peças e/ou componentes eletrônicos ou mecânicos, as peças substituídas deverão ser originais do fabricante e ter especificações iguais ou superiores às substituídas;

5.2.8. As peças e componentes trocados deverão ser novos – não utilizados ou recondicionados;

5.2.9. O primeiro atendimento dos chamados técnicos deverá ser presencial e feito nas dependências da sede do Tribunal Regional Eleitoral do Paraná (on site) em Curitiba, de segunda-feira a sexta-feira, no horário das 12h30m às 18h30m, por profissionais especializados

5.2.10. Quando não for possível a solução do problema no local, sendo

necessária a remoção do equipamento, o conserto deverá ser efetivado nas dependências do laboratório da Contratada, ficando a mesma responsável pelo translado dos equipamentos e sua devolução em perfeitas condições de uso;

5.2.11. A Contratada deverá manter, durante os 24 (vinte e quatro) meses de vigência da garantia, e às suas expensas, central de atendimento para abertura de chamados técnicos pelo menos no horário das nove às dezoito horas, de segunda a sexta-feira. A central deverá ser acionada preferencialmente por e-mail. Será aceita também a disponibilização de canal para abertura de chamados técnicos por meio de telefone ou serviço web da contratada;

5.2.12. Na abertura do chamado técnico, a Contratada deverá fornecer um número de registro único para cada chamado;

5.2.13. Considerar-se-á como recebida a solicitação de abertura do chamado técnico após o envio do e-mail (levando em consideração a data e hora do envio do e-mail) ou da abertura da ocorrência/ordem por telefone ou no serviço web da contratada (este último deve gerar um protocolo de atendimento com as informações de número da ordem de serviço, descrição do pedido de suporte e data e hora da abertura do chamado técnico);

5.2.14. A contratada deverá entregar, obrigatoriamente, para o fiscal setorial da contratação ao final de todo atendimento realizado um laudo contendo, no mínimo, as seguintes informações:

- 5.2.14.1. Data e hora da abertura do chamado;
- 5.2.14.2. Número de registro do chamado;
- 5.2.14.3. Número do patrimônio TRE-PR do equipamento envolvido;
- 5.2.14.4. Número de série do equipamento envolvido;
- 5.2.14.5. Data e hora da chegada do técnico no local de atendimento para o primeiro atendimento;
- 5.2.14.6. Data e hora da resolução do problema, se aplicável;
- 5.2.14.7. Procedimentos realizados;
- 5.2.14.8. No caso de substituição de peças, a descrição do componente substituído.

5.2.15. A contratada deverá encaminhar para o gestor da garantia técnica, através do e-mail rede@tre-pr.jus.br, no prazo máximo de 24 (vinte e quatro) horas após a realização dos atendimentos, uma cópia do laudo deixado com o fiscal da contratação ao final de cada visita técnica.

5.2.16. A Contratada deverá encaminhar mensalmente, até o 5º (quinto) dia útil do mês subsequente, relatório de todos os chamados técnicos, atendidos ou não, realizados em sua central de atendimento no mês anterior. O relatório deverá conter, pelo menos, as seguintes informações:

- 5.2.16.1. Data e hora da abertura dos chamados;
- 5.2.16.2. Número de registro dos chamados;
- 5.2.16.3. Número do patrimônio TRE-PR dos equipamentos envolvidos;
- 5.2.16.4. Número de série dos equipamentos envolvidos;
- 5.2.16.5. Data e hora da chegada do técnico nos locais de atendimento;
- 5.2.16.6. Data e hora das resoluções dos problemas, quando aplicável;
- 5.2.16.7. No caso de substituição de peças, a descrição dos componentes substituídos.

5.2.17. Caso constatado, durante a vigência do contrato, repetidos defeitos em

um mesmo componente dentro do lote dos equipamentos adquiridos, principalmente na placa principal, disco rígido ou fonte de alimentação, relacionados à preexistência de algum vício de conhecimento superveniente à data de sua aquisição, a Contratada será, a critério da Contratante, obrigada a trocar o componente de todos os equipamentos fornecidos;

5.2.18. A contratada deverá, durante a vigência do contrato, prestar todas as informações solicitadas pelos gestores, esclarecendo dúvidas, inclusive, dando todo o suporte necessário no que tange a levantamentos e estudos referentes ao objeto da contratação, no prazo máximo de 05 (cinco) dias úteis.

5.2.19. A instituição poderá promover, a qualquer tempo, diligência para checar a veracidade das informações prestadas pela contratada e ainda verificar por amostragem a confrontação do detalhamento das especificações técnicas do Termo de Referência com os equipamentos recebidos.

5.2.20. Constatada alguma irregularidade, a qualquer tempo, a contratada deverá saná-la no prazo máximo de 05 (cinco) dias úteis.

5.3. OUTRAS OBRIGAÇÕES

5.3.1. Todos os equipamentos a serem entregues deverão ser idênticos.

5.3.2. Todas as funcionalidades e/ou licenciamentos descritos para os itens 1, 2 e 3 deste pregão deverão estar licenciados no modelo perpétuo, mantendo as funcionalidades descritas em operação de forma independente da vigência do contrato de garantia dos equipamentos;

5.3.3. A Contratada, para o caso de equipamentos, deve garantir que todos os componentes do produto são novos (sem uso, reforma ou recondicionamento) e que não estarão fora de linha de fabricação durante a validade do registro de preço. Será permitida a oferta de equipamentos comprovadamente similares, pelo mesmo preço, no caso de indisponibilidade do originalmente proposto, ficando à critério da contratante o aceite ou não do equipamento ofertado.

5.3.4. Todos os cabos e conectores externos necessários ao funcionamento dos equipamentos deverão ser fornecidos com comprimento de 1,5m (um metro e cinquenta centímetros). Os cabos de conexão do equipamento à rede elétrica deverão seguir o padrão NBR-14136;

5.3.5. Para todos os itens de especificação serão aceitas ofertas de qualquer componente de especificação diferente da solicitada, desde que comprovadamente igual ou superior, individualmente, quanto à qualidade, o desempenho, a operacionalidade, a ergonomia ou a facilidade no manuseio do originalmente especificado – conforme o caso, e desde que não cause, direta ou indiretamente, incompatibilidade com qualquer das demais especificações, ou desvantagem nestes mesmos atributos dos demais componentes ofertados.

5.3.6. É de responsabilidade da Contratada o perfeito fornecimento do objeto, devendo ser de primeira qualidade, obedecendo à garantia legal e às demais normas do Código de Defesa do Consumidor.

5.3.7. Manter durante toda a execução do contrato, as obrigações assumidas na licitação

6. DA GESTÃO E FISCALIZAÇÃO DA CONTRATAÇÃO

6.1. Nos termos do art. 117 da Lei nº 14.133/2021, será designado representante para acompanhar e fiscalizar a entrega dos bens, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização de falhas ou defeitos observados.

7. DA PROTEÇÃO DE DADOS

7.1. A CONTRATADA declara ter ciência da existência da Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), e se compromete a adequar todos os procedimentos internos ao disposto na legislação com o intuito de proteger os dados pessoais a que venha ter acesso no cumprimento das obrigações contratuais;

7.2. As partes devem cumprir fielmente o disposto na Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei nº 13.709/2018, na Resolução TSE nº 23.644/2021 (Política de Segurança a Informação da Justiça Eleitoral), na Resolução TSE nº 23.650/2021 (Política Geral de Privacidade e Proteção de Dados Pessoais no âmbito da Justiça Eleitoral), no que couber, bem como observar as normas e diretrizes relacionadas à Segurança da Informação e Comunicações, em especial a ISO 27.001 e ISO 27.701, assim como a todos os normativos internos da CONTRATANTE relacionadas à segurança da informação e à proteção de dados pessoais.

7.3. A CONTRATADA dará conhecimento formal aos seus empregados e colaboradores que atuarão na prestação dos serviços objeto deste contrato, acerca das obrigações e condições acordadas e dos atos normativos referidos na cláusula anterior.

7.4. A CONTRATADA deverá informar, na assinatura do contrato, os dados referentes ao seu encarregado de proteção de dados (Lei nº 13.709/2018 – artigo 41), como nome, endereço eletrônico e telefones de contato.

7.5. O Encarregado da CONTRATADA manterá contato formal com o Encarregado do CONTRATANTE sempre que necessário para a formalização de demandas ou o esclarecimento de dúvidas;

7.6. A critério do Encarregado de Dados do CONTRATANTE, a CONTRATADA poderá ser provocada a colaborar na elaboração do relatório de impacto à proteção de dados pessoais (RIPD);

7.7. É vedado o compartilhamento dos dados pessoais coletados ou repassados em razão da execução do contrato com terceiros, bem como sua utilização para finalidade distinta daquela do objeto da contratação, sob pena de responsabilização administrativa, civil e criminal;

7.7.1. Na hipótese de se verificar que o cumprimento do contrato dependa da transferência, compartilhamento e/ou recebimento de dados pessoais, a CONTRATADA se compromete a informar ao CONTRATANTE, por escrito, com antecedência de, no mínimo, 15 (quinze) dias úteis, para que este autorize expressa, formal e previamente a referida prática;

7.7.2. Sem prejuízo do disposto acima, caso o CONTRATANTE autorize a subcontratação de determinados serviços a favor de terceiros que impliquem no fornecimento de dados pessoais referidos nesta cláusula, a CONTRATADA se compromete a celebrar, antes da subcontratação, um acordo de confidencialidade dos dados com a subcontratada, bem como a estender contratualmente a ela todas as suas obrigações

relativas ao tratamento de dados pessoais previstas neste contrato;

7.8. As partes se comprometem a manter sigilo e confidencialidade de todas as informações – em especial os dados pessoais e os dados pessoas sensíveis – repassados em decorrência da execução contratual, em consonância com o disposto na Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei nº 13.709/2018;

7.9. Todos os colaboradores da CONTRATADA que vierem a ter acesso à rede de computadores do CONTRATANTE, a sistemas da Justiça Eleitoral ou a documentos físicos que contenham dados pessoais para a execução de suas atividades deverão assinar um Termo de Sigilo e Responsabilidade, o qual deverá ser entregue ao fiscal do contrato antes do início da prestação de serviço de cada colaborador;

7.10. A CONTRATADA se compromete a isentar o CONTRATANTE de qualquer demanda administrativa, judicial ou extrajudicial relacionada ao descumprimento das suas obrigações no que se refere ao tratamento de dados pessoais, previstas no Contrato e na Lei nº 13.709/2018;

7.11. De acordo Com o art. 42 da LGPD, as partes responderão solidariamente, em caso de causarem danos patrimoniais, morais, individual ou coletivo, aos titulares de dados pessoais, repassados em decorrência da execução contratual, por inobservância ao que a Lei estabelece, e aquele que reparar o dano ao titular terá o direito de regresso contra os demais responsáveis;

7.12. O CONTRATANTE tem direito ao acesso às informações sobre o tratamento de seus dados, que serão disponibilizadas de forma clara, adequada e ostensiva, mediante solicitação;

7.13. Em caso de exposição/vazamento de dados ou qualquer incidente que implique violação ou risco de violação de dados pessoais as partes deverão adotar os seguintes procedimentos:

7.13.1. Na hipótese de verificação por parte do CONTRATANTE, este obriga-se a comunicar o fato imediatamente à CONTRATADA, para que tome as providencias cabíveis e necessárias no prazo máximo de 2 (dois) dias;

7.13.2. Na hipótese de verificação por parte da CONTRATADA, esta obriga-se a cientificar o CONTRATANTE no prazo de 24 (vinte e quatro) horas e a adotar as providencias cabíveis e necessárias no prazo máximo de 2 (dois) dias;

7.14. Em ambos os casos, a CONTRATADA deverá comunicar documentadamente ao CONTRATANTE as providências adotadas, a extensão dos eventuais danos e todas as informações relevantes sobre o incidente.

7.15. Uma vez terminado o contrato, a CONTRATADA obriga-se, expressamente, a excluir todo e qualquer dado pessoal tratado para a finalidade de sua execução, inclusive backups e arquivos externos, isentando o CONTRATANTE de responsabilidade por qualquer dano e prejuízo, direto ou indireto, advindos de tratamento de dados pessoais perpetrados após o término.

7.15.1. Caso exista legislação específica que preveja o armazenamento dos dados em tempo superior ao deste contrato, a contratada deve cientificar a contratante antes de fazer qualquer exclusão, mantendo os dados armazenados pelo período legal requerido.

7.16. A não observância das normas relativas à privacidade de dados pessoais, no contexto da Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei nº 13.709/2018 e dos demais normativos mencionados neste contrato, caracteriza falta e enseja MULTA DE 10% do valor total do contrato.

8. DAS DISPOSIÇÕES GERAIS

8.1. Os throughputs, capacidade de encaminhamento de informações para esta solução, devem ser comprovados por documento de domínio público do fabricante.

8.2. Dúvidas poderão ser sanadas com a Seção de Rede, por meio do telefone (041) 3330-8628 no horário compreendido entre as 12h e as 19h ou pelo e-mail rede@tre-pr.jus.br