APÊNDICE “A”

Requisitos Técnicos Mínimos e Obrigatórios da Solução

| **GRUPO** | **ITEM** | **TIPO** | **CÓDIGO** | **DESCRIÇÃO** | **MÉTRICA** | **PERÍODO**  **DE GARANTIA** | **FORMA DE**  **PAGAMENTO** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 1 | SOFTWARE | 111490 | Solução de Gerenciamento. | Unidade | 60 meses. | Unica |
| 2 | SOFTWARE | 111490 | Solução de Controle de Acesso à Rede. | Unidade | 60 meses. | Unica |
| 3 | MATERIAL | 481771 | Switch Spine. | Unidade | 60 meses. | Unica |
| 4 | MATERIAL | 481771 | Switch Leaf. | Unidade | 60 meses. | Unica |
| 5 | MATERIAL | 481771 | Switch de Distribuição. | Unidade | 60 meses. | Unica |
| 6 | MATERIAL | 393273 | Switch de Acesso. | Unidade | 60 meses. | Unica |
| 7 | MATERIAL | 462427 | GBIC 1 Gbps. | Unidade | 60 meses. | Unica |
| 8 | MATERIAL | 462427 | GBIC 10 Gbps. | Unidade | 60 meses. | Unica |
| 9 | MATERIAL | 462427 | GBIC 25 Gbps. | Unidade | 60 meses. | Unica |
| 10 | MATERIAL | 462427 | GBIC 40 Gbps. | Unidade | 60 meses. | Unica |
| 11 | MATERIAL | 462427 | GBIC 100 Gbps. | Unidade | 60 meses. | Unica |
| 12 | MATERIAL | 393275 | Controladora Wireless. | Conjunto | 60 meses. | Unica |
| 13 | MATERIAL | 393277 | Ponto de Acesso WiFi 6. | Unidade | 60 meses. | Unica |
| 14 | SERVIÇO | 111490 | Solução de Gestão de Usuário WiFi. | Unidade | 60 meses. | Unica |
| 15 | SERVIÇO | 24970 | Serviços de Capacitação. | Unidade | 03 meses. | Unica |

Tabela 01 – Escopo de Fornecimento de bens e serviços.

# item 1 - Solução de Gerenciamento.

## Ser do mesmo fabricante responsável por todos os equipamentos ofertados para este termo, sendo eles switches e pontos de acesso. Alternativamente, será permitido o uso de Solução de Controle de Acesso à Rede de empresas que possuam acordo formal de interoperabilidade que garanta a operação e evolução conjunta dos componentes da solução de gerenciamento.

## Pode ser ofertado através de uma única aplicação ou através do conjunto de softwares/módulos integrados.

## Implantar solução como appliance físico ou através de appliance virtual. No caso de appliance virtual, a contratada deverá obrigatoriamente garantir compatibilidade ou fornecer o hardware necessário para a sua implementação. Para appliance físico, a contratada deve fornecer todos os hardware e componentes para o perfeito funcionamento.

## Implantar solução de gerenciamento de forma centralizado através interface web, com hierárquica estruturada, permitindo configurar e modificar individualmente ou em grupos os switches.

## Implantar módulo de inventário que apresente informações de hardware e software dos equipamentos gerenciados.

## Implantar funcionalidade para visualização da topologia da rede e dos links existentes.

## Implantar mapa lógico da rede com ícones gráficos representando os switches, diferenciados por cores conforme o status operacional.

## Implantar administração centralizada sendo possível configurar, monitorar, adicionar e gerenciar dispositivos de forma individualizada ou através de grupo.

## Implantar mecanismos para cópia e recuperação das configurações dos equipamentos, com recursos para comparação de versões e agendamento de backups diários, semanais e mensais.

## Implantar gerenciamento das versões anteriores dos arquivos de configuração dos switches.

## Implantar funcionalidades para visualizar, comparar, agendar, executar e aplicar backups das configurações dos switches.

## Implantar armazenamento de firmwares dos equipamentos para fins de atualização.

## Implantar autenticação de administradores utilizando LDAP ou RADIUS.

## Permitir no mínimo cinco acessos/sessões administrativas simultâneas.

## Implantar múltiplos perfis para usuários com privilégios administrativos.

## Permitir a integração com servidores internos ou externos de SYSLOG.

## Implantar alertas em tempo real com indicação do nível de severidade dos eventos da rede.

## Implantar geração de alarmes com base em traps SNMP ou mensagens SYSLOG.

## Implantar detecção de falhas nos switches por meio do monitoramento de suas condições operacionais.

## Implantar envio de notificações por e-mail em caso de alarmes.

## Implantar suporte aos protocolos SSH, HTTPS, SFTP, SNMP v1-v2c-v3, MIB II (RFC1213)

## Implantar integração com plataformas de terceiros via API RESTful, permitindo requisições por HTTPS protegida por usuário e senha, bem como por token com expiração por tempo e coleta de dados dos Switches, Controladoras e Access Points e Rádios dos Pontos de Acesso.

## Implantar módulo de análise de tráfego com licenciamento para no mínimo dois coletores, compatível com SFlow, NetFlow, IPFIX ou NetStream, permitindo armazenamento, processamento e visualização dos dados em tabelas e gráficos.

### Implantar o monitoramento dos fluxos de tráfego da rede, identificando distribuição, tipos e características, com possibilidade de criação e personalização de dashboards.

### Implantar a separação do tráfego gerado por dispositivos, interfaces e endereços IP específicos.

## Permitir a geração de relatórios com dados dos switches gerenciados, com periodicidade diária, semanal, mensal, semestral e anual, incluindo exportação para planilhas em Excel, PDF e/ou Word, além da criação de regras para envio automático por e-mail.

## Possuir licenciamento com uso permanente (perpétuo) e garantia estendida de 60 meses, ou em modelo de subscrição pelo mesmo período.

## Possuir licenciamento que contemple a operação e gestão de todos os switches, controladora de rede sem fio e pontos de acesso fornecidos. Alternativamente, o licenciamento pode ser ofertado com cada equipamento individualmente.

# item 2 - Solução de Controle de Acesso à Rede.

## Ser do mesmo fabricante responsável por todos os equipamentos ofertados para este termo, sendo eles switches e pontos de acesso. Alternativamente, será permitido o uso de Solução de Controle de Acesso à Rede de empresas que possuam acordo formal de interoperabilidade que garanta a operação e evolução conjunta dos componentes da solução.

## Não serão considerados válidos sistemas que utilizem software de código aberto (open source) com finalidade genérica.

## Possuir licenciamento que permita o controle de acesso de, no mínimo, 6.000 (seis mil) dispositivos. Alternativamente, esse licenciamento pode estar distribuído entre os Switches e Access Points, proporcionalmente ao total de dispositivos suportados por cada equipamento. Conceito de Dispositivos: qualquer tipo de equipamento que possa ser conectado à rede via porta Ethernet e que exija controle de acesso, como computadores (desktops ou notebooks), impressoras de rede, pontos de acesso sem fio, telefones IP, entre outros.

## Possuir compatibilidade total para fins de gerenciamento e configuração com a controladora de rede sem fio e ponto de acesso especificados neste termo de Referência.

## Implantar solução como appliance físico ou através de appliance virtual. No caso de appliance virtual, a contratada deverá obrigatoriamente garantir compatibilidade ou fornecer o hardware necessário para a sua implementação. Para appliance físico, a contratada deve fornecer todos os hardware e componentes para o perfeito funcionamento.

## Implantar soluções de autenticação e criptografia que protejam todos os acessos administrativos.

## Permitir o gerenciamento remoto da plataforma por meio de uma interface gráfica via navegador, utilizando o protocolo seguro HTTPS.

## Permitir a validação dos responsáveis pela autorização através de diretórios externos, como Microsoft AD ou LDAP, com atribuição de permissões conforme o perfil.

## Permitir a definição de políticas com base em grupos do Microsoft AD, incluindo suporte à leitura de grupos aninhados com profundidade mínima de três níveis até os objetos finais.

## Implantar uma solução centralizada para configurar e controlar o acesso de usuários e dispositivos à rede.

## Suportar os protocolos EAP e PEAP para autenticação segura.

## Suportar, no mínimo, os seguintes métodos de autenticação em conjunto com o controlador WiFi: WPA2-PSK, WPA2-Enterprise com 802.X e WPA3-Enterprise.

## Implantar autenticação de usuários por meio de credenciais administradas (usuário e senha), redes sociais como Facebook® ou Instagram® ou LinkedIn®, e acesso automático sem cadastro prévio.

## Implantar servidor RADIUS e relay RADIUS, com capacidade de integração a servidores RADIUS externos.

## Permitir a customização da página de login dos usuários, incluindo textos, logotipo e seleção de idioma durante o processo de autenticação.

## Implantar separação do tráfego de rede dos usuários com base no tipo de autenticação realizada.

## Implantar políticas de qualidade de serviço (QoS) baseadas no perfil de autenticação dos usuários.

## Implantar mecanismos de identificação automática de dispositivos, utilizando técnicas como MAC OUI, DHCP e HTTP User-Agent.

## Implantar funcionalidades de classificação automática para criação de perfis de dispositivos, permitindo sua descoberta, categorização e agrupamento.

## Implantar varredura da rede utilizando a ferramenta NMAP.

## Implantar geração e armazenamento de registros de auditoria que permitam rastrear todas as ações nos componentes da solução, contendo evento, data/hora, usuário e IP do dispositivo.

## Implantar identificação de usuários e dispositivos conectados, exibindo nome, MAC address, status da última tentativa de acesso e tempo de conexão, tanto em redes de camada 2 quanto de camada 3 do modelo OSI.

## Implantar bloqueio de acesso à rede para dispositivos que não estejam em conformidade com as políticas de controle de acesso.

## Implantar funcionalidades para geração de relatórios gráficos com dados como fabricante, tipo de dispositivo, IP, políticas aplicadas, sistema operacional e regras de acesso.

## Possuir licenciamento permanente ou por subscrição(com cobertura de 60 (sessenta) meses).

# REQUISITOS comuns:

## Os requisitos comuns se aplicam aos ITENS: 3 - SWITCH SPINE DE 40/100 GBPS, 4 - SWITCH LEAF DE 10/25 GBPS, 5 - SWITCH DE DISTRIBUIÇÃO.

## Possuir arquitetura do tipo Chassis Modular ou Switch Standalone. Para a arquitetura **Chassis Modular**, deve estar equipada com placas supervisoras e de switch fabric em configuração redundante. Implantar capacidade de virtualização que permita consolidar, no mínimo, duas unidades físicas em uma única instância lógica. Além disso, incluir pelo menos quatro slots exclusivos para interfaces de rede. Para a arquitetura **Switch Standalone**, o equipamento deve contar com arquitetura distribuída para gerenciamento e processamento, com suporte à formação de cluster virtual composto por, no mínimo, duas unidades físicas operando como uma única instância lógica.

## Possuir padrão físico compatível com racks de 19 polegadas, ocupando 1 unidade de altura (1RU), e incluir os itens e acessórios necessários para a instalação.

## Para atender à quantidade de portas e à capacidade exigida, é permitida a oferta de até dois switches. Caso sejam fornecidas duas unidades, estas devem ser conectadas por link de 100GE, utilizando porta adicional às previstas no total solicitado.

## Fornecer 1 (um) cabo AOC (QSFP28/QSFP28) de 100GE com comprimento mínimo de 1 metro para viabilizar a formação de cluster virtual com outra unidade. Alternativamente, permitir essa conexão por meio de interfaces ópticas de 100GE e cordão óptico de 1 ou 2 metros.

## Possuir indicadores luminosos (LEDs) específicos para cada uma das funções descritas a seguir, com capacidade de sinalizar: a) o estado operacional do switch, b) a identificação do switch como master da pilha, c) o funcionamento individual das fontes de alimentação, d) o status de cada porta de rede, e, e) o equipamento que requer manutenção, com possibilidade de acionamento remoto do LED específico para facilitar sua localização.

## Possuir fontes de alimentação internas, redundantes no modelo N+1, independentes, compatíveis com tensões de 110–220V AC e frequência de 50/60 Hz, com suporte a troca em funcionamento (hot-swap) e fluxo de ar do tipo “Front-to-Back”. Todos os compartimentos de fonte devem estar ocupados.

## Possuir módulos de ventilação internos (fan tray), redundantes, independentes entre si, com capacidade de troca em funcionamento (hot-swap). Todos os slots destinados aos ventiladores devem estar preenchidos.

## Implantar capacidade para, no mínimo, 4.000 VLANs ativas.

## Possuir conformidade com os padrões IEEE: 802.3x, 802.1d, 802.1w, 802.1s (mínimo 64 instâncias), 802.1p (mínimo 8 filas por porta), 802.1q, 802.1x, 802.3ad (mínimo 8 portas por grupo).

## Implantar funcionalidades de roteamento estático e protocolos para IPv4 e IPv6, OSPF e OSPFv3 e BGP e BGP4+.

## Implantar suporte aos protocolos IGMP nas versões v1, v2 e v3 com funcionalidade de snooping/proxy.

## Implantar suporte a encapsulamento de VLANs utilizando Q-in-Q ou VXLAN.

## Implantar protocolos de multicast (PIM-SM ou PIM-SSM) e PIM-DM.

## Implantar funcionalidade de relay para DHCPv4 e DHCPv6.

## Implantar gerenciamento dos switches através das interfaces e protocolos a seguir: porta RS-232, USB, SNMP Trap, SNMP v1/v2c/v3, NetConf ou scripts em Python, MIB I ou II, RMON com suporte a quatro grupos ou telemetria, FTP ou TFTP, NTP ou SNTP, Command Line interface, Telnet, SSHv2, IPv4/IPv6.

## Permitir a aplicação de listas de controle de acesso (ACLs) com intuito de restringir conexões via Telnet e SSH.

## Permitir múltiplas versões/releases de firmware.

## Implementar mecanismos AAA (Autenticação, Autorização e Contabilização) para controle de acesso.

## Implementar protocolo de monitoramento entre switches que permita a desativação automática de uma porta ao identificar falha na comunicação entre os dispositivos.

## Suportar ativação futura de funcionalidades de EVPN, VXLAN e Telemetria.

## Implantar ferramenta de análise da qualidade das conexões de rede, com suporte mínimo aos testes de ICMP (echo/reply), TCP (syn/syn-ack), UDP jitter e ICMP jitter.

## Implantar suporte a pelo menos um dos protocolos de coleta de fluxo de tráfego a seguir: NetFlow, Sflow, NetStream, IPFIX (RFC 3917).

## Implantar funcionalidade de espelhamento de porta (Port Mirror) nas seguintes modalidades: entrada, saída e entrada/saída simultaneamente.

## Implantar listas de controle de acesso (ACLs) em nível de hardware, sendo baseadas em endereços MAC de origem/destino, portas ipv4/v6 TCP/UDP e endereços IP v4/v6 de origem/destino.

## Implantar mecanismos de agendamento de prioridade como Strict Priority (SP/PQ) e algoritmos de distribuição como WRR, WFQ ou DRR.

## Implantar classificação de tráfego considerando as camadas 2, 3 e 4 do modelo OSI.

## Implantar funcionalidades de políticas de roteamento e roteamento baseado em políticas (Policy-Based Routing)..

## Implantar bloqueio de pacotes do tipo unicast desconhecido, broadcast e multicast.

## Implantar proteção contra ataques ARP spoofing e flooding, inundações do tipo SYN e UDP.

## Implantar recurso de anti-spoofing que utilize dinamicamente a tabela de roteamento, sem necessidade de listas de acesso, com configuração por interface.

## Permitir controle sobre o número de endereços MAC aprendidos, com limitação conforme necessidade da rede.

## Implantar proteção baseada em BPDU (root/loop), visando prevenir loops e preservar a integridade da topologia.

## Implantar suporte ao protocolo TACACS+ (ou equivalente) ou RADIUS.

## Possuir nível de proteção IP20 ou superior, conforme classificação de resistência à entrada de objetos sólidos e contato acidental.

## Possuir homologação Anatel emitido pelo fabricante e correspondente ao modelo ofertado.

# requisitos específicos: item 3 - Switch Spine

## Possuir no mínimo 36 (trinta e seis) interfaces 40/100GE, QSFP28 Frontais.

## Implantar performance mínima de switching de 7.2 Tbps.

## Possuir memória Flash de, no mínimo, 4 GB.

## Possuir memória RAM de, no mínimo, 8 GB.

## Permitir armazenamento simultâneo de múltiplas imagens do sistema operacional, possibilitando atualizações de software sem a exclusão das versões anteriores.

## Implantar escalabilidade para, no mínimo, 250.000 rotas FIB IPv4.

## Implantar escalabilidade para, no mínimo, 125.000 rotas FIB IPv6.

## Implantar escalabilidade para, no mínimo, 256.000 entradas MAC.

## Implantar escalabilidade para, no mínimo, 256 grupos VRRP/VRRP6.

# requisitos específicos: item 4 - Switch

## Possuir no mínimo 48 (quarenta e oito) interfaces 1/10/25GE, SFP28 Frontais.

## Possuir no mínimo 8 (oito) interfaces 40/100GE, QSFP28 frontais.

## Implantar performance mínima de switching de 4 Tbps.

## Possuir memória Flash de, no mínimo, 4 GB.

## Possuir memória RAM de, no mínimo, 8 GB.

## Permitir armazenamento simultâneo de múltiplas imagens do sistema operacional, possibilitando atualizações de software sem a exclusão das versões anteriores.

## Implantar escalabilidade para, no mínimo, 250.000 rotas FIB IPv4.

## Implantar escalabilidade para, no mínimo, 125.000 rotas FIB IPv6.

## Implantar escalabilidade para, no mínimo, 256.000 entradas MAC.

## Implantar escalabilidade para, no mínimo, 256 grupos VRRP/VRRP6.

# REQUISITOS ESPECÍFICOS: item 5 - Switch de Distribuição.

## Possuir no mínimo 48 (quarenta e oito) interfaces 1/10GE, SFP+ Frontais.

## Possuir no mínimo 6 (seis) interfaces 40/100GE, QSFP28 frontais.

## Implantar performance mínima de switching de 2.1 Tbps.

## Possuir memória Flash de, no mínimo, 2 GB.

## Possuir memória RAM de, no mínimo, 4 GB.

## Permitir armazenamento simultâneo de múltiplas imagens do sistema operacional, possibilitando atualizações de software sem a exclusão das versões anteriores.

## Implantar escalabilidade para, no mínimo, 64.000 rotas FIB IPv4.

## Implantar escalabilidade para, no mínimo, 64.000 rotas FIB IPv6.

## Implantar escalabilidade para, no mínimo, 96.000 entradas na tabela MAC.

## Implantar escalabilidade para, no mínimo, 60 grupos VRRP/VRRP6.

## Implantar suporte ao padrão IEEE 802.1X para autenticação de usuários e dispositivos, com integração ao servidor RADIUS, oferecendo suporte aos métodos EAP: CHAP, PAP, PEAP, TLS e TTLS. Permitir a criação de regras de acesso sem autenticação, viabilizando a disponibilização de serviços mínimos, como portal cativo ou servidores de atualização, antes da autenticação bem-sucedida. Também é necessário suportar a associação dinâmica de usuários/dispositivos a VLANs específicas, utilizando os atributos RADIUS Tunnel-Type, Tunnel-Medium-Type e Tunnel-Private-Group-ID, além da atribuição de listas de controle de acesso (ACLs) por usuário e grupo, com suporte ao atributo RADIUS Filter-Id.

## Implantar adicionalmente mecanismos de reautenticação, incluindo reautenticação 802.1X, reautenticação periódica com configuração personalizada, reautenticação pontual por endereço MAC, e reautenticação baseada nos atributos Session-Timeout e Termination-Action. Também deve permitir realizar reautenticação para usuários em estado de autenticação não realizada, com tentativas periódicas em casos de falha, pré-conexão ou indisponibilidade temporária do servidor RADIUS.

## Implantar mecanismos de logout para usuários autenticados via IEEE 802.1X, incluindo a detecção automática da desconexão, com exclusão da entrada correspondente e notificação ao servidor RADIUS para encerramento da contabilização; suporte ao logout por meio de pacotes EAPoL-Logoff e resposta EAP-Failure; desconexão por comando administrativo e por mecanismos automáticos de detecção de inatividade, como handshake-period e handshake-times; além do logout via Disconnect Message (DM), com aplicação dos atributos RADIUS Session-Timeout e Termination-Action.

## Implantar mecanismos de temporização para o processo de autenticação IEEE 802.1X, garantindo controle eficiente de retransmissões, falhas e tentativas excessivas, contemplando temporizador de solicitação de identidade (EAP-Request/Identity), com configuração do intervalo de retransmissão e número máximo de tentativas, de desafio de autenticação EAP baseado em MD5 (EAP-Request/MD5 Challenge), encerrando as tentativas após o limite configurado e de silêncio, permitindo configurar período em que usuários que excedam número de falhas consecutivas em curto intervalo de tempo sejam bloqueados de novas tentativas de autenticação. Caso ocorra a falha na autenticação 802.1X após o tempo configurado, permitir autenticação por endereço MAC (MAC Authentication Bypass – MAB)

## Implantar IEEE 802.1x para autenticação de usuários/dispositivos com suporte a múltiplos suplicantes por porta.

## Implantar autenticação por endereço MAC (MAC Authentication Bypass – MAB), com integração ao servidor RADIUS, garantindo controle de autorização e aplicação de políticas de acesso, contemplando o suporte aos protocolos PAP e CHAP, a criação de regras de acesso sem autenticação, permitindo disponibilizar serviços mínimos, como portal cativo ou servidores de atualização, antes da autenticação bem-sucedida do dispositivo, a associação dinâmica do dispositivo a VLAN específica, com suporte a RADIUS Tunnel-Type, Tunnel-Medium-Type e Tunnel-Private-Group-ID, a atribuição de ACLs por dispositivo após autenticação, com suporte a RADIUS Filter-Id, para grupos de dispositivos após autenticação, com suporte a RADIUS Filter-Id e a reautenticação MAC, periódica configurável, pontual por endereço MAC, baseada nos atributos Session-Timeout e Termination-Action e baseado em usuários com estado de autenticação não realizada, incluindo tentativas periódicas de reautenticação em casos de falha, pré-conexão ou indisponibilidade temporária do servidor RADIUS.

## Implantar mecanismos de logout para dispositivos autenticados por endereço MAC (MAC Authentication Bypass – MAB), garantindo a imediata liberação de recursos de sessão e a atualização do servidor RADIUS, contemplando a detecção automática da desconexão de dispositivos, de forma que o equipamento exclua a entrada correspondente e notifique o servidor RADIUS para encerrar a contabilização, a desconexão por comando administrativo, bem como por mecanismos automáticos de detecção de inatividade, incluindo handshake-period e handshake-times e o logout mediante Disconnect Message (DM), bem como à aplicação de Session-Timeout e Termination-Action.

## Implantar temporizador de silêncio para autenticação por endereço MAC (MAC Authentication Bypass – MAB), com garantia à detecção de falhas consecutivas de autenticação em curto período de tempo e a aplicação automática de período de silêncio, durante o qual o equipamento deverá rejeitar novas tentativas de autenticação do dispositivo.

## Implantar autenticação via portal web (Portal Authentication), garantindo a interação entre cliente, dispositivo de acesso, servidor de portal externo e servidor de autenticação, contemplando a autenticação do usuário em página web HTTPS, com suporte a personalização das páginas de autenticação, permitindo a criação de regras de acesso sem autenticação, afim de disponibilizar serviços mínimos, como portal cativo ou servidores de atualização, antes da autenticação bem-sucedida do dispositivo, dever ser possível a atribuição de ACLs por dispositivo após autenticação, com suporte a RADIUS Filter-Id e a atribuição de ACLs para grupos de dispositivos após autenticação, com suporte a RADIUS Filter-Id.

## Implantar mecanismos de logout para usuários/dispositivos autenticados via portal web (Portal Authentication), garantindo a imediata liberação de recursos de sessão e a atualização do servidor RADIUS, contemplando a detecção automática da desconexão de usuários/dispositivos, de forma que o equipamento exclua a entrada correspondente e notifique o servidor RADIUS para encerrar a contabilização, o logout iniciado pelo cliente (Client-Initiated Logout), no qual o usuário envia uma solicitação de desconexão à página de portal, o logout mediante (Disconnect Message – DM) ou pela utilização de RADIUS Session-Timeout e Termination-Action e o logout iniciado pelo servidor de portal.

## Implantar suporte a autenticação em múltiplos modos (Multi-mode Authentication), com a integração entre IEEE 802.1X e autenticação por endereço MAC (MAC Authentication Bypass – MAB), permitindo uso de MAC quando 802.1X não for bem-sucedido, com a autenticação via portal web (Portal Authentication) com prioridade de autenticação por MAC (MAC-Address Prioritized Portal), redirecionando o usuário à página web apenas em caso de falha do MAC e com o cache de endereços MAC no servidor RADIUS, permitindo reconexão automática de terminais autenticados anteriormente dentro do período de validade configurado

## Implantar suporte a autenticação de pontos de acesso (Access Points – APs) como clientes IEEE 802.1X, garantindo sua autenticação, com suporte a métodos de autenticação como EAP-PEAP e EAP-TLS, incluindo o uso de perfis dedicados de cliente 802.1X e o carregamento de certificados digitais quando necessário.

# item 6 - Switch de acesso

## Possuir indicadores luminosos (LEDs) específicos para cada uma das funções descritas a seguir, com capacidade de sinalizar: a) o estado operacional do switch, b) a identificação do switch como master da pilha, c) o funcionamento individual das fontes de alimentação, d) o status de cada porta de rede, e, e) o equipamento que requer manutenção, com possibilidade de acionamento remoto do LED para facilitar sua localização.

## Possuir no mínimo 2 (duas) fontes de energia internas, independentes, redundantes entre si, bi-volt (110V / 220V), cabos de alimentação NBR 14.136 e com tecnologia hot-swap. As fontes em conjunto, devem prover no mínimo, 1.500 (Mil e quinhentos) Watts de potência para POE independente da tensão de entrada.

## Possuir pelo menos 2 (duas) unidades de ventilação (FANs) para garantir o resfriamento adequado do equipamento.

## Possuir no mínimo 48 interfaces Ethernet 10/100/1000Base-T com conectores RJ-45, compatíveis com os padrões IEEE 802.3af e IEEE 802.3at.

## Possuir no mínimo 4 portas SFP+ de 10 Gigabit Ethernet, operando de forma independente das portas anteriores, totalizando 52 interfaces ativas simultaneamente.

## Implantar performance mínima de switching de 216 Gbps.

## Possuir memória Flash de, no mínimo, 1 GB.

## Possuir memória RAM de, no mínimo, 2 GB.

## Permitir armazenamento simultâneo de múltiplas imagens do sistema operacional, possibilitando atualizações de software sem a exclusão das versões anteriores.

## Implantar escalabilidade para, no mínimo, 32.000 entradas MAC.

## Implantar escalabilidade para, no mínimo, 4.000 VLANs ativas e no mínimo, 1.000 interfaces de VLAN.

## Implantar gerenciamento unificado como uma única entidade lógica através de empilhamento de, no mínimo, 8 (oito) switches.

## Cada equipamento deve oferecer performance de empilhamento agregado de no mínimo 40 Gbps em modo Full Duplex.

## O conjunto deve ser entregue com cabo de empilhamento de, no mínimo, 10 Gbps e 1 metro de comprimento, utilizando portas adicionais e dedicadas, com suporte à redundância.

## Possuir conformidade com os padrões IEEE: 802.3x, 802.1d, 802.1w, 802.1s (mínimo 64 instâncias), 802.1p (mínimo 8 filas por porta), 802.1q, 802.1x, 802.3ad (mínimo 8 portas por grupo e 20 grupos).

## Implementar funcionalidade associada ao Spanning Tree que permita configurar portas de acesso (utilizadas por estações de trabalho) para que entrem diretamente no estado de encaminhamento (Forwarding), sem passar pelos estados de escuta e aprendizado (Listening-Learning), mantendo a capacidade de detecção de loops na rede.

## Implantar funcionalidades de roteamento estático e protocolos para IPv4 e IPv6, OSPF, OSPFv3, BGP, BGP4+, RIPv1 ou RIPv2, VRRP e VRRP6, com suporte para no mínimo 60 grupos.

## Implantar suporte aos protocolos IGMP nas versões v1, v2 e v3 com funcionalidade de snooping.

## Implantar os protocolos LLDP e LLDP-MED para descoberta e gerenciamento de dispositivos na rede.

## Implantar suporte a encapsulamento de VLANs utilizando Q-in-Q ou VXLAN.

## Implantar protocolos de multicast PIM-SM ou PIM-SSM e PIM-DM.

## Implantar servidor DHCPv4/v6 com funcionalidade que restrinja a atribuição de endereços IP apenas a servidores previamente autorizados (Trusted Server).

## Implantar funcionalidade de relay para DHCPv4 e DHCPv6.

## Implantar gerenciamento dos switches através das interfaces e protocolos a seguir: porta RS-232, USB, SNMP Trap, SNMP v1/v2c/v3, NetConf ou scripts em Python, MIB I ou II, RMON com suporte a quatro grupos ou telemetria, FTP ou TFTP, NTP ou SNTP, Command Line interface, Telnet, SSHv2, IPv4/IPv6.

## Permitir a aplicação de listas de controle de acesso (ACLs) com intuito de restringir conexões via Telnet e SSH.

## Permitir mecanismos de AAA (Autenticação, Autorização e Contabilização) para controle de acesso.

## Implementar protocolo de monitoramento entre switches que permita a desativação automática de uma porta ao identificar falha na comunicação entre os dispositivos.

## Suportar ativação futura de funcionalidades de telemetria.

## Implantar ferramenta de análise da qualidade das conexões de rede, com suporte mínimo aos testes de ICMP (echo/reply), TCP (syn/syn-ack), UDP jitter e ICMP jitter.

## Implantar suporte a pelo menos um dos protocolos de coleta de fluxo de tráfego a seguir: NetFlow, Sflow, NetStream, IPFIX (RFC 3917).

## Implantar funcionalidade de espelhamento de porta (Port Mirror) nas seguintes modalidades: entrada, saída e entrada/saída simultaneamente.

## Implantar listas de controle de acesso (ACLs) em nível de hardware, sendo baseadas em endereços MAC de origem/destino, portas ipv4/v6 TCP/UDP e endereços IP v4/v6 de origem/destino.

## Permitir escalabilidade de no mínimo 2.000 regras em ACL para protocolo IPV4 e 2.000 regras em ACL para protocolo IPV6.

## Implantar mecanismos de agendamento de prioridade como Strict Priority (SP ou PQ) e algoritmos de distribuição (WRR ou WFQ ou DRR).

## Implantar classificação de tráfego considerando as camadas 2, 3 e 4 do modelo OSI.

## Implantar funcionalidades de políticas de roteamento e roteamento baseado em políticas (Policy-Based Routing).

## Implantar bloqueio de pacotes do tipo unicast desconhecido, broadcast e multicast.

## Implantar proteção contra ataques ARP spoofing e flooding, inundações do tipo SYN e UDP.

## Implantar recurso de anti-spoofing que utilize dinamicamente a tabela de roteamento, sem necessidade de listas de acesso, com configuração por interface.

## Permitir controle sobre o número de endereços MAC aprendidos, com limitação conforme necessidade da rede.

## Implantar suporte ao protocolo TACACS+ (ou equivalente) ou RADIUS.

## Implantar suporte ao padrão IEEE 802.1X para autenticação de usuários e dispositivos, com integração ao servidor RADIUS, oferecendo suporte aos métodos EAP: CHAP, PAP, PEAP, TLS e TTLS. Permitir a criação de regras de acesso sem autenticação, viabilizando a disponibilização de serviços mínimos, como portal cativo ou servidores de atualização, antes da autenticação bem-sucedida. Também é necessário suportar a associação dinâmica de usuários/dispositivos a VLANs específicas, utilizando os atributos RADIUS Tunnel-Type, Tunnel-Medium-Type e Tunnel-Private-Group-ID, além da atribuição de listas de controle de acesso (ACLs) por usuário e grupo, com suporte ao atributo RADIUS Filter-Id.

## Implantar adicionalmente mecanismos de reautenticação, incluindo reautenticação 802.1X, reautenticação periódica com configuração personalizada, reautenticação pontual por endereço MAC, e reautenticação baseada nos atributos Session-Timeout e Termination-Action. Também deve permitir realizar reautenticação para usuários em estado de autenticação não realizada, com tentativas periódicas em casos de falha, pré-conexão ou indisponibilidade temporária do servidor RADIUS.

## Implantar mecanismos de logout para usuários autenticados via IEEE 802.1X, incluindo a detecção automática da desconexão, com exclusão da entrada correspondente e notificação ao servidor RADIUS para encerramento da contabilização; suporte ao logout por meio de pacotes EAPoL-Logoff e resposta EAP-Failure; desconexão por comando administrativo e por mecanismos automáticos de detecção de inatividade, como handshake-period e handshake-times; além do logout via Disconnect Message (DM), com aplicação dos atributos RADIUS Session-Timeout e Termination-Action.

## Implantar mecanismos de temporização para o processo de autenticação IEEE 802.1X, garantindo controle eficiente de retransmissões, falhas e tentativas excessivas, contemplando temporizador de solicitação de identidade (EAP-Request/Identity), com configuração do intervalo de retransmissão e número máximo de tentativas, de desafio de autenticação EAP baseado em MD5 (EAP-Request/MD5 Challenge), encerrando as tentativas após o limite configurado e de silêncio, permitindo configurar período em que usuários que excedam número de falhas consecutivas em curto intervalo de tempo sejam bloqueados de novas tentativas de autenticação. Caso ocorra a falha na autenticação 802.1X após o tempo configurado, permitir autenticação por endereço MAC (MAC Authentication Bypass – MAB)

## Implantar IEEE 802.1x para autenticação de usuários/dispositivos com suporte a múltiplos suplicantes por porta.

## Implantar autenticação por endereço MAC (MAC Authentication Bypass – MAB), com integração ao servidor RADIUS, garantindo controle de autorização e aplicação de políticas de acesso, contemplando o suporte aos protocolos PAP e CHAP, a criação de regras de acesso sem autenticação, permitindo disponibilizar serviços mínimos, como portal cativo ou servidores de atualização, antes da autenticação bem-sucedida do dispositivo, a associação dinâmica do dispositivo a VLAN específica, com suporte a RADIUS Tunnel-Type, Tunnel-Medium-Type e Tunnel-Private-Group-ID, a atribuição de ACLs por dispositivo após autenticação, com suporte a RADIUS Filter-Id, para grupos de dispositivos após autenticação, com suporte a RADIUS Filter-Id e a reautenticação MAC, periódica configurável, pontual por endereço MAC, baseada nos atributos Session-Timeout e Termination-Action e baseado em usuários com estado de autenticação não realizada, incluindo tentativas periódicas de reautenticação em casos de falha, pré-conexão ou indisponibilidade temporária do servidor RADIUS.

## Implantar mecanismos de logout para dispositivos autenticados por endereço MAC (MAC Authentication Bypass – MAB), garantindo a imediata liberação de recursos de sessão e a atualização do servidor RADIUS, contemplando a detecção automática da desconexão de dispositivos, de forma que o equipamento exclua a entrada correspondente e notifique o servidor RADIUS para encerrar a contabilização, a desconexão por comando administrativo, bem como por mecanismos automáticos de detecção de inatividade, incluindo handshake-period e handshake-times e o logout mediante Disconnect Message (DM), bem como à aplicação de Session-Timeout e Termination-Action.

## Implantar temporizador de silêncio para autenticação por endereço MAC (MAC Authentication Bypass – MAB), com garantia à detecção de falhas consecutivas de autenticação em curto período de tempo e a aplicação automática de período de silêncio, durante o qual o equipamento deverá rejeitar novas tentativas de autenticação do dispositivo.

## Implantar autenticação via portal web (Portal Authentication), garantindo a interação entre cliente, dispositivo de acesso, servidor de portal externo e servidor de autenticação, contemplando a autenticação do usuário em página web HTTPS, com suporte a personalização das páginas de autenticação, permitindo a criação de regras de acesso sem autenticação, afim de disponibilizar serviços mínimos, como portal cativo ou servidores de atualização, antes da autenticação bem-sucedida do dispositivo, dever ser possível a atribuição de ACLs por dispositivo após autenticação, com suporte a RADIUS Filter-Id e a atribuição de ACLs para grupos de dispositivos após autenticação, com suporte a RADIUS Filter-Id.

## Implantar mecanismos de logout para usuários/dispositivos autenticados via portal web (Portal Authentication), garantindo a imediata liberação de recursos de sessão e a atualização do servidor RADIUS, contemplando a detecção automática da desconexão de usuários/dispositivos, de forma que o equipamento exclua a entrada correspondente e notifique o servidor RADIUS para encerrar a contabilização, o logout iniciado pelo cliente (Client-Initiated Logout), no qual o usuário envia uma solicitação de desconexão à página de portal, o logout mediante (Disconnect Message – DM) ou pela utilização de RADIUS Session-Timeout e Termination-Action e o logout iniciado pelo servidor de portal.

## Implantar suporte a autenticação em múltiplos modos (Multi-mode Authentication), com a integração entre IEEE 802.1X e autenticação por endereço MAC (MAC Authentication Bypass – MAB), permitindo uso de MAC quando 802.1X não for bem-sucedido, com a autenticação via portal web (Portal Authentication) com prioridade de autenticação por MAC (MAC-Address Prioritized Portal), redirecionando o usuário à página web apenas em caso de falha do MAC e com o cache de endereços MAC no servidor RADIUS, permitindo reconexão automática de terminais autenticados anteriormente dentro do período de validade configurado

## Implantar suporte a autenticação de pontos de acesso (Access Points – APs) como clientes IEEE 802.1X, garantindo sua autenticação, com suporte a métodos de autenticação como EAP-PEAP e EAP-TLS, incluindo o uso de perfis dedicados de cliente 802.1X e o carregamento de certificados digitais quando necessário.

## Possuir nível de proteção IP20 ou superior, conforme classificação de grau de proteção contra entrada de objetos sólidos e contato acidental.

## Possuir homologação Anatel emitido em nome do fabricante e correspondente ao modelo ofertado.

# item 7 - GBIC 1 Gbps

## Módulo GBIC do tipo óptico compatível com o padrão 1000Base-SX, utilização de fibra multimodo, com alcance de até 550 metros ou Módulos GBIC do tipo elétrico compatível com o padrão 1000BASE-T, utilização de cabo par trançado, com alcance de até 100 metros.

## Fornecer cordão óptico duplex, multimodo, com comprimento de 2,0 metros, conectores LC/LC, para o padrão 1000BASE-SX ou patch cord CAT6, com comprimento de 2,0 metros, para o padrão 1000BASE-T, ambos montados e certificados diretamente pelo fabricante responsável.

## O Módulo GBIC deve ser obrigatoriamente do fabricante dos switches.

## No ato da emissão da OFB a CONTRATANTE vai definir o padrão, 1000BaseSX ou 1000BaseT, desejado para a interface.

# item 8 - GBIC 10 Gbps

## Módulo GBIC óptico do tipo SFP+, compatível com o padrão 10GE Base-SR, utilização de fibra multimodo, com alcance de até 300 metros.

## Fornecer cordão óptico duplex, multimodo, com comprimento de 2,0 metros, conectores LC/LC, montado e certificado diretamente pelo fabricante responsável.

## O Módulo GBIC óptico deve ser obrigatoriamente do fabricante dos switches.

# item 9 - GBIC 25 GBPS

## Módulo GBIC óptico do tipo SFP28, compatível com o padrão 25GE Base-SR, utilização de fibra multimodo, com alcance de até 100 metros.

## Fornecer cordão óptico duplex, multimodo, com comprimento de 2,0 metros, conectores LC/LC, montado e certificado diretamente pelo fabricante responsável.

## O Módulo GBIC óptico deve ser obrigatoriamente do fabricante dos switches.

# item 10 - GBIC 40 GBPS

## Módulo GBIC óptico do tipo QSFP+, compatível com o padrão 40GE, fibra multimodo, até 100 metros.

## Fornecer cordão óptico duplex, multimodo, com comprimento de 2,0 metros, conectores LC/LC ou MPO/MPO ou MPT/MPT, montado e certificado diretamente pelo fabricante responsável.

## O Módulo GBIC óptico deve ser obrigatoriamente do fabricante dos switches.

# item 11 - GBIC 100 GBPS

## Módulo GBIC óptico do tipo QSFP28, compatível com o padrão 100GE, fibra multimodo, até 100 metros.

## Fornecer cordão óptico duplex tipo multimodo com comprimento de 2,0 metros, equipado com conectores LC/LC ou MPO/MPO ou MPT/MPT, montado e certificado diretamente pelo fabricante responsável.

## O Módulo GBIC óptico deve ser obrigatoriamente do fabricante dos switches.

# item 12 - CONTROLADORa WIRELESS

## Possuir arquitetura baseada em hardware dedicado exclusivamente à administração de pontos de acesso compatíveis com WiFi 6.

## Fornecer conjunto com no mínimo 2 (dois) e no máximo 3 (três) controladores WiFi, configurados em redundância N + 1, garantindo continuidade operacional.

## Permitir operação em alta disponibilidade tanto de hardware quanto de software, operando em modo ativo-passivo.

## Pode ser ofertado switches redundantes com desempenho equivalente ou superior ao dos controladores, para executar funções de camada 2 (switching) e camada 3 (routing).

## Fornecer licenças para a gestão do total de pontos de acesso ofertados.

## Possuir o número máximo de fontes de alimentação instaladas, 110-220V, 50/60Hz, redundantes e hot swapping, número máximo de módulos de ventilação (Fan Trail) instalados redundantes, hot swapping e com fluxo de ar front-to-back.

## Possuir padrão físico compatível com racks de 19 polegadas, ocupando 1 unidade de altura (1RU).

## Possuir 02 portas de 40GbaseSR QSFP+ ou 08 portas de 10GbaseSR SFP+, com possibilidade de agregação.

## Implantar performance de encaminhamento de 100 Gbps em modo tunelado.

## Implantar escalabilidade de no mínimo 4.000 VLANs no padrão IEEE 802.1q.

## Permitir escalabilidade de 10.000 usuários Wi-Fi.

## Permitir escalabilidade de 500 SSIDs.

## Implantar escalabilidade de 1.000 listas de controle de acesso.

## Suportar a possibilidade de expansão futura da capacidade de gerenciamento, contemplando até 2.000 Pontos de Acesso (APs).

## Implantar recursos de roteamento dos tipos: estático IPv4 e IPv6, OSPF, OSPFv3 e VRRP.

## Implantar protocolos de DHCP Server, Relay e Snooping.

## Implantar mecanismo de identificação automática de Pontos de Acesso, com distinção baseada nas camadas de roteamento da rede.

## Implantar modo de operação em que o tráfego dos usuários seja redirecionado ao controlador antes de atingir a rede local.

## Implantar modo de operação em que os pontos de acesso realizem o chaveamento local do tráfego dos usuários.

## Implantar a tecnologia WDS (Wireless Distribution System).

## Implantar tecnologia de direcionamento de sinal (Beamforming).

## Implantar mecanismo de transição rápida entre pontos de acesso (fast-roaming).

## Implantar suporte ao padrão Hotspot 2.0.

## Implantar mecanismo de balanceamento de carga entre os pontos de acesso.

## Implantar método de priorização de frequência.

## Implantar controle operacional para pontos de acesso em modo mesh e não-mesh.

## Implantar suporte ao protocolo WEP e negociação de chaves EAPOL-Key.

## Implantar autenticação via PSK, WPA com TKIP e WPA2 com AES/CCMP.

## Implantar padrão WPA3 com criptografia AES de 128 e 256 bits.

## Implantar autenticação com geração de chaves criptográficas dinâmicas e estáticas.

## Implantar segurança conforme padrão IEEE 802.11i, incluindo WIPS, Black List e White List.

## Implantar solução para mitigação de ataques como AP spoofing, broadcast de desautenticação, client flood, rogue APs, entre outros.

## Implantar AAA (Autenticação, Autorização e Accounting) e protocolo RADIUS Authentication, Accounting e Extensions.

## Implantar interface de linha de comando (CLI), suporte a HTTPS e acesso remoto via SSHv2.

## Implantar sincronização de horário via NTP ou SNTP.

## Implantar suporte aos protocolos SNMPv1, SNMPv2c e SNMPv3, com coleta via MIB II.

## Implantar mecanismos de controle de tráfego como Traffic Shaping e Policing, com suporte ao IEEE 802.1p.

## Implantar funcionalidades do padrão WMM (Wireless Multimedia Extensions) conforme IEEE 802.11e.

## Implantar controle e limites de utilização de banda por usuário e por SSID, com classificação de tráfego por IP, portas e MAC.

## Implantar suporte ao padrão IEEE 802.1X para autenticação de usuários e dispositivos, com integração ao servidor RADIUS, oferecendo suporte aos métodos EAP: CHAP, PAP, PEAP, TLS e TTLS. Permitir a criação de regras de acesso sem autenticação, viabilizando a disponibilização de serviços mínimos, como portal cativo ou servidores de atualização, antes da autenticação bem-sucedida. Também é necessário suportar a associação dinâmica de usuários/dispositivos a VLANs específicas, utilizando os atributos RADIUS Tunnel-Type, Tunnel-Medium-Type e Tunnel-Private-Group-ID, além da atribuição de listas de controle de acesso (ACLs) por usuário e grupo, com suporte ao atributo RADIUS Filter-Id.

## Implantar adicionalmente mecanismos de reautenticação, incluindo reautenticação 802.1X, reautenticação periódica com configuração personalizada, reautenticação pontual por endereço MAC, e reautenticação baseada nos atributos Session-Timeout e Termination-Action. Também deve permitir realizar reautenticação para usuários em estado de autenticação não realizada, com tentativas periódicas em casos de falha, pré-conexão ou indisponibilidade temporária do servidor RADIUS.

## Implantar mecanismos de logout para usuários autenticados via IEEE 802.1X, incluindo a detecção automática da desconexão, com exclusão da entrada correspondente e notificação ao servidor RADIUS para encerramento da contabilização; suporte ao logout por meio de pacotes EAPoL-Logoff e resposta EAP-Failure; desconexão por comando administrativo e por mecanismos automáticos de detecção de inatividade, como handshake-period e handshake-times; além do logout via Disconnect Message (DM), com aplicação dos atributos RADIUS Session-Timeout e Termination-Action.

## Implantar mecanismos de temporização para o processo de autenticação IEEE 802.1X, garantindo controle eficiente de retransmissões, falhas e tentativas excessivas, contemplando temporizador de solicitação de identidade (EAP-Request/Identity), com configuração do intervalo de retransmissão e número máximo de tentativas, de desafio de autenticação EAP baseado em MD5 (EAP-Request/MD5 Challenge), encerrando as tentativas após o limite configurado e de silêncio, permitindo configurar período em que usuários que excedam número de falhas consecutivas em curto intervalo de tempo sejam bloqueados de novas tentativas de autenticação. Caso ocorra a falha na autenticação 802.1X após o tempo configurado, permitir autenticação por endereço MAC (MAC Authentication Bypass – MAB)

## Implantar IEEE 802.1x para autenticação de usuários/dispositivos com suporte a múltiplos suplicantes por porta.

## Implantar autenticação por endereço MAC (MAC Authentication Bypass – MAB), com integração ao servidor RADIUS, garantindo controle de autorização e aplicação de políticas de acesso, contemplando o suporte aos protocolos PAP e CHAP, a criação de regras de acesso sem autenticação, permitindo disponibilizar serviços mínimos, como portal cativo ou servidores de atualização, antes da autenticação bem-sucedida do dispositivo, a associação dinâmica do dispositivo a VLAN específica, com suporte a RADIUS Tunnel-Type, Tunnel-Medium-Type e Tunnel-Private-Group-ID, a atribuição de ACLs por dispositivo após autenticação, com suporte a RADIUS Filter-Id, para grupos de dispositivos após autenticação, com suporte a RADIUS Filter-Id e a reautenticação MAC, periódica configurável, pontual por endereço MAC, baseada nos atributos Session-Timeout e Termination-Action e baseado em usuários com estado de autenticação não realizada, incluindo tentativas periódicas de reautenticação em casos de falha, pré-conexão ou indisponibilidade temporária do servidor RADIUS.

## Implantar mecanismos de logout para dispositivos autenticados por endereço MAC (MAC Authentication Bypass – MAB), garantindo a imediata liberação de recursos de sessão e a atualização do servidor RADIUS, contemplando a detecção automática da desconexão de dispositivos, de forma que o equipamento exclua a entrada correspondente e notifique o servidor RADIUS para encerrar a contabilização, a desconexão por comando administrativo, bem como por mecanismos automáticos de detecção de inatividade, incluindo handshake-period e handshake-times e o logout mediante Disconnect Message (DM), bem como à aplicação de Session-Timeout e Termination-Action.

## Implantar temporizador de silêncio para autenticação por endereço MAC (MAC Authentication Bypass – MAB), com garantia a detecção de falhas consecutivas de autenticação em curto período de tempo e a aplicação automática de período de silêncio, durante o qual o equipamento deverá rejeitar novas tentativas de autenticação do dispositivo.

## Implantar autenticação via portal web (Portal Authentication), garantindo a interação entre cliente, dispositivo de acesso, servidor de portal externo e servidor de autenticação, contemplando a autenticação do usuário em página web HTTPS, com suporte a personalização das páginas de autenticação, permitindo a criação de regras de acesso sem autenticação, afim de disponibilizar serviços mínimos, como portal cativo ou servidores de atualização, antes da autenticação bem-sucedida do dispositivo, dever ser possível a atribuição de ACLs por dispositivo após autenticação, com suporte a RADIUS Filter-Id e a atribuição de ACLs para grupos de dispositivos após autenticação, com suporte a RADIUS Filter-Id.

## Implantar mecanismos de logout para usuários/dispositivos autenticados via portal web (Portal Authentication), garantindo a imediata liberação de recursos de sessão e a atualização do servidor RADIUS, contemplando a detecção automática da desconexão de usuários/dispositivos, de forma que o equipamento exclua a entrada correspondente e notifique o servidor RADIUS para encerrar a contabilização, o logout iniciado pelo cliente (Client-Initiated Logout), no qual o usuário envia uma solicitação de desconexão à página de portal, o logout mediante (Disconnect Message – DM) ou pela utilização de RADIUS Session-Timeout e Termination-Action e o logout iniciado pelo servidor de portal.

## Implantar base de dados interna dedicada ao registro de usuários visitantes, com capacidade mínima para armazenar 4.000 cadastros distintos.

## Os requisitos técnicos podem ser atendidos em conjunto com a documentação referente ao ITEM 12 – Ponto de Acesso.

## Possuir homologação Anatel emitido em nome do fabricante e correspondente ao modelo ofertado.

# item 13 - Ponto de Acesso WiFi 6

## Implantar Access Point WiFi 6 gerenciado pelo ITEM 11 - CONTROLADORA DE REDE SEM FIO.

## Permitir gerenciamento centralizado por meio de Controlador compatível com WiFi 6.

## Os requisitos técnicos podem ser atendidos em conjunto com a documentação referente ao ITEM 11 - CONTROLADORA DE REDE SEM FIO.

## Possuir indicador luminoso (LED) que sinalize o estado operacional do ponto de acesso.

## Suportar a instalação de mecanismo de proteção contra furto, com estrutura compatível para dispositivo tipo Kensington ou equivalente.

## Possuir todos os itens e acessórios necessários para sua instalação em teto e parede.

## Permitir alimentação elétrica via Power over Ethernet conforme IEEE 802.3af ou 802.3at, e suporte à instalação futura de fonte AC 220V ou DC 12V.

## Possuir uma porta Ethernet 10/100/1000BaseT com auto-sensing, auto MDI/MDX e conector RJ-45 fêmea.

## Permitir a conexão de dispositivos IoT via porta USB, com compatibilidade para RFID e Zigbee.

## Implantar tecnologia Bluetooth Low Energy (BLE) versão 5.2 ou superior.

## Possuir antenas internas, não visíveis, com tecnologia de banda dupla (2,4/5,0 GHz), padrão omnidirecional.

## Possuir pico de ganho por antena de 4 dBi (2,4 GHz), 4 dBi (BLE) e 5 dBi (5,0 GHz).

## Possuir ganho médio das antenas de 2 dBi (2,4 GHz) e 3 dBi (5,0 GHz).

## Implantar performance de transmissão de até 570 Mbit/s na faixa de 2,4 GHz.

## Implantar performance de transmissão de até 1,2 Gbit/s na faixa de 5,0 GHz.

## Implantar performance de transmissão total de 1,77 Gbit/s por ponto de acesso.

## Permitir performance de conexões simultâneas de no mínimo, 350 usuários por rádio.

## Implantar suporte para até 16 SSIDs distintos por rádio.

## Implantar tecnologia MIMO 2x2:2 com múltiplos fluxos espaciais na frequência de 5,0 GHz.

## Implantar configuração MIMO 2x2:2 com múltiplos fluxos espaciais na frequência de 2,4 GHz.

## Implantar compatibilidade com os padrões IEEE 802.11ax, 802.11a/b/g/n/ac e ac wave 2.

## Implantar tecnologias como OFDMA, MRC e DFS.

## Permitir configuração que viabilize conexões simultâneas de dispositivos nas bandas de 2,4 GHz e 5 GHz.

## Implantar suporte ao uso de intervalo de guarda curto (SGI) nas larguras de canal de 20 MHz, 40 MHz e 80 MHz.

## Implantar suporte às tecnologias 1024 QAM, Beamforming, CDD, CSD, DFS, MRC, STBC, LDPC, U-APSD e OFDMA.

## Implantar cliente DHCP e mecanismos de segurança como DHCP Snooping.

## Implantar níveis de autenticação do tipo “Enterprise” para WPA2 e WPA3.

## Implementar padrão WPA3 com criptografia AES nos formatos de 128 bits e 256 bits.

## Suportar configuração que permita a conexão de dispositivos Wi-Fi e operação como sensor WIPS na mesma frequência do canal utilizado pelo rádio do Access Point.

## Permitir atualização remota do sistema operacional do equipamento.

## Implantar ajuste automático de potência de transmissão e seleção de canal de rádio.

## Implantar escolha inteligente e automática do canal de operação.

## Implantar modos de encaminhamento de tráfego tanto tunelado (tunnel mode) quanto local (local forward).

## Possuir homologação Anatel emitida em nome do fabricante e correspondente ao modelo ofertado.

# item 14 - Software de gestão de usuário WiFi.

## Implantar plataforma de gerenciamento de usuários da rede Wi-Fi, contemplando funcionalidades completas de identificação, autenticação, autorização e contabilização de acessos.

## Cada unidade contratada deverá corresponder a um período de 60 meses de subscrição, habilitando o uso da plataforma para um ponto de acesso específico. Não deve haver qualquer limitação quanto ao número de usuários conectados, simultaneamente ou não, exceto aquelas decorrentes das restrições técnicas dos equipamentos de rede.

## Permitir armazenamento dos registros de conexão dos usuários por um período mínimo de 60 meses.

## Possuir arquitetura baseada em computação em nuvem, com infraestrutura resiliente contra ataques DDoS e proteção por firewall de aplicação web (WAF).

## Permitir operação da plataforma por, no mínimo, dois provedores estabelecidos no território nacional ou, alternativamente, por um único provedor com duas zonas de disponibilidade independentes.

## Possuir estrutura multi-inquilino (multi-tenancy), assegurando o isolamento completo entre o ambiente da CONTRATANTE e demais organizações.

## Possuir conformidade com a Lei Geral de Proteção de Dados (LGPD) e com o Marco Civil da Internet.

## Disponibilizar telas de acesso aos usuários nos idiomas português (Brasil) e inglês (Americano).

## Permitir apresentação de termo de uso ao usuário, com leitura obrigatória e aceite prévio à liberação da conexão.

## Permitir edição dos termos de uso conforme as necessidades específicas da CONTRATANTE.

## Permitir personalização do layout das telas de acesso, permitindo aplicação da identidade visual da CONTRATANTE.

## Ser compatível com os sistemas operacionais Android, iOS® e Microsoft®, garantindo ampla acessibilidade.

## Ser compatível com os navegadores Safari®, Chrome®, Internet Explorer e Firefox®, assegurando interoperabilidade.

## Possuir layout responsivo, adaptável automaticamente às resoluções de notebooks, desktops, tablets e smartphones.

## Ser compatível com o controlador Wi-Fi e os pontos de acesso fornecidos neste processo licitatório.

## Implantar autenticação de usuários via integração com pelo menos três das seguintes plataformas: Facebook®, LinkedIn®, Instagram®, Twitter® e Google®.

## Implantar autenticação de usuários via integração com a plataforma Gov.BR (https://sso.acesso.gov.br), utilizando os tokens de acesso fornecidos pela CONTRATANTE.

## Implantar autenticação via auto registro, por meio de formulário customizável, permitindo a coleta de dados como nome, e-mail, CPF, data de nascimento e telefone, com validações apropriadas.

## Implantar autenticação via integração com LDAP e Captive Portal, com suporte aos protocolos RADIUS Authentication e Accounting.

## Implantar reconhecimento de usuários recorrentes, permitindo acesso automático mediante identificação do dispositivo móvel.

## Implantar liberação de acesso por endereço MAC, com cadastro manual ou dinâmico para dispositivos previamente conectados.

## Permitir configuração do período de disponibilidade do serviço, com definição de horários e dias da semana.

## Permitir gestão de tempo de uso, com definição de limite diário e tempo máximo de inatividade, utilizando dados obtidos via protocolo RADIUS Accounting.

## Permitir, quando a identificação, autenticação, autorização e contabilidade ocorrer via rede social, que o portal administrativo exiba dados públicos do perfil social do usuário/visitante.

## Possuir múltiplos perfis administrativos com diferentes níveis de permissão.

## Permitir exportação de dados da plataforma.

## Implantar visualização gráfica de acessos, sistemas operacionais, dispositivos e SSIDs.

## Permitir emissão de relatórios com base nos dados de conexão dos usuários, extraídos da infraestrutura Wi-Fi via protocolo RADIUS Accounting.

## Permitir integração com sistemas externos via WebService REST/API.

# item 15 - Serviços de Capacitação.

## Os serviços de capacitação técnica online deverão contemplar a explanação teórica para administradores da solução.

## Cada 1 (uma) unidade de serviço permite a capacitação de até 4 pessoas.

## A CONTRATADA deve apresentar cronograma da capacitação técnica e caso a CONTRATANTE não concorde com as datas e horários propostos pela CONTRATADA, o cronograma deverá ser planejado em comum acordo entre as partes.

## A capacitação técnica deve ser realizada nas dependências da CONTRATANTE e/ou ONLINE, com carga horária de 24 horas distribuídas em aulas de 8 horas diárias, em data e horário a ser definido entre as partes.

## Após o término dos serviços a CONTRATADA deverá fornecer certificados da capacitação técnica realizada.

## Conteúdo programático:

### Arquitetura de funcionamento dos produtos.

### Configuração básica para funcionamento.

### Configuração de gerenciamento.

## **ENTREGÁVEL**: A CONTRATADA disponibilizará à CONTRATANTE o relatório da execução da capacitação técnica com os seguintes dados: a) Nome do participante, b) Conteúdo da capacitação, c) Data e Hora, d) Carga horaria, e) Frequência.

# CONDIÇÕES GERAIS DE EXECUÇÃO DOS SERVIÇOS DE GARANTIA E SUPORTE

## Os serviços deverão ser prestados pela CONTRATADA ou por representante indicada pela CONTRATADA ou pela fabricante dos produtos, sem prejuízo a responsabilidade integral da CONTRATADA quanto aos atendimentos dos níveis de serviço. O prazo de garantia e suporte para cada item do fornecimento está expresso na tabela "**Tabela 01 - Escopo de Fornecimento**", coluna "**PERÍODO DE GARANTIA**".

## Entende-se por “**Garantia**” ou “**Suporte**” ou “**Manutenção**”, doravante denominada unicamente como “**Garantia**”, toda atividade do tipo “corretiva” não periódica que variavelmente poderá ocorrer, durante todo o período de garantia. Possui suas causas em falhas e erros no Software/Hardware e trata da correção dos problemas atuais e não iminentes de. Exclui-se da garantia defeitos que não tenham sua origem comprovada na fabricação dos produtos. Esta “Garantia” inclui os procedimentos destinados a recolocar em perfeito estado de operação os serviços e produtos ofertados, tais como:

### **Do hardware**: Configuração ou reconfiguração decorrente de falhas de fabricação no hardware, fornecimento de peças de reposição, substituição de hardware defeituoso por defeito de fabricação, atualização da versão de drivers e firmwares, correção de defeitos de fabricação, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados.

### **Do software**: Configuração ou reconfiguração decorrente de falhas de desenvolvimento do software, atualização da versão de software, correção de defeitos de desenvolvimento do software, de acordo com os manuais e as normas técnicas específicas do fabricante para os recursos utilizados.

### **Quanto às atualizações pertinentes aos softwares**: Entende-se como “atualização” o provimento de toda e qualquer evolução de software, incluindo correções, “patches”, “fixes”, “updates”, “service packs”, novas “releases”, “versions”, “builds”, “upgrades”, abrangendo inclusive versões não sucessivas, nos casos em que a solicitação de atualização de tais versões ocorra durante o período de garantia do contrato.

## A CONTRATADA fornecerá e aplicará pacotes de correção, em data e horário a serem definidos pela CONTRATANTE, sempre que forem encontradas falhas de laboratório (bugs) ou falhas comprovadas de segurança em software ou firmware dos aparelhos que integrem o objeto do contrato. O atendimento deste requisito está condicionado a liberação pelo fabricante dos pacotes de correção e/ou novas versões de software.

## É facultado a CONTRATADA a execução, ao seu planejamento e disponibilidade, de “Garantia” do tipo “preventiva” que pela sua natureza reduza a incidência de problemas que possam gerar “Garantia” do tipo “corretiva”. As manutenções do tipo “preventiva” não podem gerar custos a CONTRATANTE.

## A manutenção técnica do tipo “corretiva” será realizada sempre que solicitada pelo CONTRATANTE por meio da abertura de chamado técnico diretamente à empresa CONTRATADA (ou a outra informada pela CONTRATADA) via telefone (com número do tipo “0800” caso a Central de Atendimento esteja fora de Brasília-DF) ou Internet ou e-mail ou fac-símile ou outra forma de contato. Os serviços de “Garantia” incluem:

### Solução de problemas relativos à indisponibilidade da solução decorrentes de problemas de fabricação e desenvolvimento.

### Solução de falhas ou defeitos no funcionamento, incluindo a instalação de arquivos para correção dos erros.

### Esclarecimento de dúvidas sobre o funcionamento e operação da solução.

### Instalação de novas versões ou atualizações e patches.

## A CONTRATADA deve disponibilizar a central atendimento 8 horas por dia, 5 dias da semana (de segunda a sexta-feira, exceto feriados) e equipe com conhecimentos sólidos no funcionamento e operação da solução de gestão.

## Os serviços de “Garantia” devem disponibilizar os seguintes tipos de atendimento:

### **Nível I - Atendimento Telefônico (Help Desk)**: chamados abertos através de ligação telefônica ou e-mail ou outra forma de contato, em regime de 8x5: 8 horas por dia, 5 dias da semana (de segunda a sexta-feira, exceto feriado). Esse serviço deve atender demandas dos usuários referentes ao funcionamento da solução, que decorram de problemas de funcionamento.

### **Nível II - Atendimento Remoto**: atendimento remoto de chamados de suporte técnico através de tecnologia disponibilizada pela CONTRATANTE, mediante prévia autorização e seguindo os padrões de segurança da CONTRATANTE, objetivando análise e solução remota dos problemas apresentados.

### **Nível III - Atendimento Presencial (On-Site)**: atendimentos técnicos realizados nas dependências do CONTRATANTE, através de visita de técnico especializado, com a finalidade de resolver demandas abertas no Help Desk e não solucionadas pelo Atendimento Telefônico e/ou Remoto. Os atendimentos serão sempre realizados na sede da CONTRATANTE em Brasília/DF, sendo este o ponto físico para o atendimento técnico on-site de qualquer necessidade de garantia e/ou suporte técnico.

## Toda “Garantia” deve ser solicitada inicialmente via Help Desk (Nível I), ficando a transferência do atendimento para o Atendimento Remoto (Nível II) condicionado à autorização da CONTRATANTE.

## Toda “Garantia” solicitada inicialmente via Help Desk (Nível I), deve ser transferida para o Atendimento Presencial (Nível II ou III) quando o atendimento do Help Desk não for suficiente para solução do problema sem a intervenção presencial de um técnico.

## Os prazos para a prestação dos serviços devem garantir a observância ao atendimento do seguinte **Acordo de Níveis de Serviços (ANS)** e sua **SEVERIDADE**:

### **SEVERIDADE URGENTE** – Solução totalmente inoperante. Prazo máximo de início de atendimento de até 04 horas úteis contadas a partir do horário de abertura do chamado.

### **SEVERIDADE IMPORTANTE** – Solução parcialmente inoperante – Necessidade de suporte na solução com a necessidade de interrupção de funcionamento da solução. Prazo máximo de início de atendimento de até 24 horas úteis contadas a partir do horário de abertura do chamado.

### **SEVERIDADE NORMAL** – Solução não inoperante, mas com problema de funcionamento – Necessidade de suporte na solução sem a necessidade de interrupção de funcionamento da solução. Prazo máximo de início de atendimento de até 48 horas úteis contadas a partir do horário de abertura do chamado.

### **SEVERIDADE EXTERNO** – Solução inoperante, de forma parcial ou total, fruto de falha de elemento de hardware e/ou software não fornecido pela CONTRATADA. Neste caso, ficam suspensos todos os prazos de atendimento até que a CONTRATANTE resolva os problemas externos que provocam a inoperância da solução. Após a CONTRATANTE disponibilizar o ambiente de forma estável para a reativação da solução, a CONTRATADA realizará avaliação da extensão do dano a solução e as partes definirão em comum acordo o prazo para a reativação da solução.

### **SEVERIDADE INFORMAÇÃO** – Solicitações de informações diversas ou dúvidas sobre a solução. Prazo máximo de resposta de até 10 dias úteis, contados a partir da data de abertura da ocorrência.

## Um chamado técnico somente poderá ser fechado após a confirmação do responsável da CONTRATANTE e o término de atendimento dar-se-á com a disponibilidade do recurso para uso em perfeitas condições de funcionamento no local onde está instalado.

## Na abertura de chamados técnicos, serão fornecidas informações, como Número de série (quando aplicável), anormalidade observada, nome do responsável pela solicitação do serviço e versão do software utilizada e **severidade** do chamado.

## A **severidade** do chamado poderá ser reavaliada quando verificado que foi erroneamente aplicada, passando a contar no momento da reavaliação os novos prazos de atendimento e solução.

## A CONTRATADA poderá solicitar a prorrogação de qualquer dos prazos para conclusão de atendimentos de chamados, desde que o faça antes do seu vencimento e devidamente justificado.

## Deve ainda, incluir as atividades necessárias para disponibilizar serviço de painéis (dashboards) executivos, com indicadores de performance, segurança, operação e administração de toda a solução, de forma que permita a CONTRATANTE monitorar a execução dos serviços prestados. deve ainda:

### Implantar o serviço no formato SaaS em nuvem ou on-premisse.

### É de responsabilidade da CONTRATADAa definição, criação e manutenção dos indicadores e painéis, de forma que a CONTRATANTE possa consumir os painéis prontos.

### Permitir acesso através de interface Web(HTTPS), com controle de acesso por identificação de usuário e solicitação de senha e duplo fator de autenticação, ambos de forma individual por usuário através de Software Token (“tokens baseados em software”).

### Possuir recurso de **“**reset” de senha, de forma que que o usuário receba por e-mail link para reset da senha ou nova senha temporária de acesso.

### Permitir o cadastramento de no mínimo 05 (usuários) da CONTRATANTE para visualização dos painéis disponibilizados.

### Possuir tecnologia do tipo responsiva, de forma que a visualização se adapte ao tamanho da tela dos dispositivos utilizados no acesso.

### Implantarcontrole de acesso por usuário, de forma a controlar o grupo de assunto ou painel que pode ser visualizado.

### Possuir a capacidade de coleta de dados de forma agendada, recorrente e automática.

### Permitir a visualização gráfica de indicadores por tabelas, KPIs, gráficos, texto formatados, através de:

#### KPIs (key performance indicators), nos formatos Rótulo/Valor, Dial com valores de destino, mínimo e máximo e discagem completo, com definição de cor de fundo e textos, tipo de fonte, tamanho de fonte, título do indicador, formatação numérica, moeda, porcentagem, casas decimais, unidade de medida e indicadores de milhar e decimal.

#### Tabelas do tipo linha x coluna, com a definição de cor de fundo e textos, tipo de fonte, tamanho de fonte, título da tabela, formatação numérica, moeda, porcentagem, casas decimais, unidade de medida e indicadores de milhar e decimal para valores das colunas.

#### Gráficos em Pizza, Pizza semicircular, Pizza Anel, Barra Horizontal e Vertical normal, Barra Horizontal e Vertical empilhada, Barra Horizontal e Vertical 100% empilhada, linha com e sem marcadores, Dispersão, Bolha normal e empilhada, Área com e sem marcadores e Área empilhada com e sem marcadores, com a definição de cor de fundo e textos, tipo de fonte, tamanho de fonte, título do gráfico, formatação numérica, moeda, porcentagem, casas decimais, unidade de medida e indicadores de milhar e decimal para valores das séries, eixos e legenda.

### Permitir filtro interno e individualizado por painel, através de: a) campos de dados, b) intervalos do tipo acima de, abaixo de, entre valor inicial e final, c) Top N e Down N, d) data através dos critérios de filtro por ano, trimestre, mês, dia, semana, dia da semana, dia do mês, data real, data e hora real, hora e intervalos entre datas.

### Permitir a exportação de indicadores gráficos no formato de imagem ou pdf.

### A Licitante deve informar a plataforma a ser utilizada, bem como apresentar comprovação do atendimento dos requisitos.

# Comprovações de atendimento dos requisitos

## Na leitura de cada requisito, devem ser observadas as seguintes definições: o termo **“suportar”** indica que a funcionalidade deve estar apta a ser implementada, seja de forma imediata ou futura, por meio de eventual aquisição de licenciamento adicional de hardware ou software. Já os termos **“permitir”, “implantar”, “possuir” e “fornecer”** determinam que a funcionalidade requerida deve estar incluída integralmente na proposta da licitante, devendo ser disponibilizada sem qualquer custo adicional ao valor ofertado.

## A licitante deverá, junto à proposta comercial, anexar a documentação que comprove o atendimento integral a cada requisito. Além disso, será necessário:

### Garantir que os produtos apresentados tenham procedência comprovada e contem com garantia oficial do fabricante em território nacional.

### Detalhar a composição completa de cada item do escopo, informando marca, modelo, códigos de identificação, descrição dos códigos, unidade de fornecimento, quantidade dos conjuntos, de modo a permitir a identificação inequívoca dos bens e serviços ofertados.

### Incluir documentação técnica oficial emitida pelo fabricante (tais como manuais, catálogos, links em site oficial ou imagens) que evidencie o atendimento a todos os requisitos técnicos. Essa comprovação deverá ser organizada em planilha ponto a ponto, com indicação do documento consultado e da página correspondente. Não serão aceitas declarações emitidas por fabricante, distribuidor ou pela própria licitante como forma de comprovação.

## A CONTRATANTE poderá realizar diligências a qualquer tempo para verificar a veracidade das informações e documentos apresentados.

**----------------FIM DO APÊNDICE “A” -----------------**