ANEXO V – WIRELESS

1. ESPECIFCAÇÕES TÉCNICAS – CONTROLADORA WIRELESS EM NUVEM

1.01 Deve ser uma plataforma licenciada e hospedada em nuvem, disponibilizada em ambiente com certificação ISO27001 ou similar, responsável por toda configuração, gerenciamento e monitoramento centralizado dos pontos de acessos WiFi capaz de suportar a criação de políticas e filtros de segurança;

1.02 Deve ser fornecido na forma Software as a Service (SaaS) hospedado na nuvem do próprio fabricante, sem depender de softwares, máquinas virtuais ou hardwares instalados no ambiente da contratante;

1.03 O funcionamento da rede não pode ser totalmente dependente da plataforma de gestão em nuvem, ou seja, quando ocorrer uma perda de comunicação com a nuvem, como falha do link, por exemplo, a rede WLAN deve permanecer operando;

1.04 Ainda em caso de perda da comunicação com a plataforma de gerência, a solução deve garantir a continuidade do acesso local e individual a cada access points via interface web durante e a após o período de indisponibilidade;

1.05 A solução deve estar pronta e licenciada para garantir o gerenciamento de no mínimo 4.000 (quatro mil) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor;

1.06 O controlador wireless na nuvem deverá ser descoberto automaticamente e manualmente pelos Access points;

1.07 A solução deve permitir a configuração de Short Guard Interval para o rádio 5GHz;

1.08 A solução deve implementar recurso de NAT no SSID, incluindo o serviço de DHCP Server para facilitar a configuração de redes visitantes. Deve ser possível especificar o endereço e máscara da rede que os clientes wireless receberão IP;

1.09 A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2);

1.10 Deve suportar e possuir solução de alta disponibilidade;

1.11 Deve possuir gerenciamento Web com interface gráfica acessível através dos principais browsers do mercado (Internet Explorer, Firefox ou Chrome) e capacidade de criação automática de topologia;

1.12 Deve suportar gerenciamento para múltiplas localidades (sites) e múltiplos usuários;

1.13 Deve implementar informações sobre os pontos de acesso e dispositivos conectados a rede com função de monitoramento e alertas;

1.14 Deve realizar atualizações de firmware dos pontos de acesso WiFi;

1.15 Deve empregar criptografia de dados no canal de comunicação com os pontos de acesso WiFi, como TLS ou SSL ou IPSEC ou CAPWAP ou DTLS ou HTTPS entre outros;

1.16 Deve disponibilizar no mínimo 03 (três) níveis de acesso administrativo à Console de Gerenciamento Web, sendo:

1.16.1 Nível 1: Acesso completo permissão total para administração da controladora;

1.16.2 Nível 2: Alterações de configurações básicas;

1.16.3 Nível 3: Acesso apenas de leitura;

1.17 Deve implementar mecanismos de 2FA(Two-factor authentication) ou outros mecanismos seguros para acesso administrativo a Console de Gerenciamento WEB;

1.18 Deve permitir a criação de múltiplos profiles de configurações permitindo assim a segmentação e agrupamento de Access Points para uma melhor organização do ambiente e otimização da gestão operacional;
1.19 Deve permitir a criação de contas de usuários para acesso a rede WiFi na própria controladora;
1.20 Deve implementar autenticação local, 802.1x e Captive portal;
1.21 Deve permitir a customização do Captive Portal, possibilitando a importação de imagens e logo;
1.22 Deve permitir a visualização de um conjunto de informações dos Access Points, disponibilizando no mínimo nome, MAC Address e endereço IP;
1.23 Deve informar a quantidade de dispositivos ou usuários conectados em cada Access Point;
1.24 Deve informar o volume de tráfego em cada Access Point e interfaces através de dashboards;
1.25 Deve fornecer relatórios e monitoramento com gráficos contendo informações sobre a os Access Points;
1.26 Permitir acesso aos Acess Points via CLI ou via Web de forma remota ou através da plataforma de gerencia em nuvem;
1.27 Deve permitir a visualização de um conjunto de informações dos dispositivos conectados à rede wireless, disponibilizando pelo menos os dados abaixo especificados:
1.27.1 Nome do usuário, Endereço IP e MAC Address;
1.27.2 Tipo de autenticação;
1.27.3 Tempo de conexão;
1.27.4 Informação de SSIDs;
1.27.5 Informação do tráfego de utilização dos usuários;
1.27.6 Qualidade do sinal dos dispositivos conectados a rede;
1.28 Deve possuir API's documentadas para fins de integrações;
1.29 Deve possuir capacidade de gerar relatórios em formatos conhecidos como .csv, .xlsx, .pdf ou similares;
1.30 Deve possibilitar o agrupamento dos Access Point suportando a criação e o gerenciamento de grupos de Access Point simultâneos, facilitando a administração dos equipamentos;
1.31 Permitir a gravação e envio de eventos por meio do protocolo syslog para no minimo dois servidores remotos;
1.32 A solução deve permitir a visualização dos logs de eventos e acessos por um período mínimo de 12 (doze) meses, permitindo consultas retroativas;
1.33 A solução deve permitir a emitir relatórios da rede e estes deverão ser enviados automaticamente via e-mail ou para uma base de gestão e armazenamento conforme agendamento que poderá ser configurado com frequência diária, semanal e mensal;
1.34 A solução deve enviar e-mails de notificação aos administradores em caso de alertas na rede;
1.35 A solução deve permitir que softwares de monitoramento realizem consultas aos pontos de acesso via protocolo SNMP, Netconf ou outros similares;
1.36 Deve implementar o protocolo NTP ou SNTP;
1.37 Implementar varredura de RF contínua ou sob demanda, com identificação de APs irregulares;
1.38 Na ocorrência de inoperância de um AP, o sistema de controle WLAN deverá ajustar automaticamente a potência dos APs adjacentes, de modo a prover a cobertura da área não assistida;
1.39 Ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF baseado em performance;
1.40 Implementar sistema de balanceamento de carga para associação de clientes entre APs próximos, para otimizar a performance da rede;
1.41 Ajustar, dinamicamente, o nível de potência e canal de rádio dos APs, de modo a otimizar o tamanho da célula de RF, garantindo a performance e escalabilidade;
1.42 Permitir conexão entre APs sem a necessidade de conexão cabeada, implementando assim uma rede padrão mesh;
1.43 Gerenciar de forma centralizada e descentralizada a autenticação de usuários;
1.44 Possuir base de dados de usuários interna para autenticação de usuários convidados / temporários (acesso guest);

1.45 Permitir autenticação de usuário utilizando RADIUS e LDAP de modo que esta integração seja feita através da controladora, do ponto de acesso ou portal web;
1.46 Realizar o provisionamento de usuários convidados (guests) através de interface Web por meio de um usuário administrativo com permissões mínimas, exclusivas para este fim;
1.47 Permitir o controle de banda disponível (traffic shaper) por usuário, por aplicação ou SSID;
1.48 Possibilitar roaming com integridade de sessão, dando suporte a aplicações em tempo real, tais como, VoIP, VoWLAN, videoconferência, dentre outras;
1.49 Deve implementar a tecnologia de "Channel load balancing", permitindo que clientes sejam automaticamente distribuídos entre Pontos de Acesso adjacentes operando em canais distintos, com o objetivo de balancear a carga entre os Pontos de Acesso;
1.50 Implementar varredura de RF para identificação de ataques e APs intrusos não autorizados (rogues);
1.51 Realizar a identificação e contenção de redes "AD-HOC";
1.52 Deve implementar funcionalidades de WIPS e WIDS para prevenção e detecção de ataques à rede sem fio possibilitando a tomada automática de ações de defesa;
1.53 Permitir configurar o bloqueio na comunicação entre os clientes wireless conectado a um determinado SSID;
1.54 Deve ser fornecida com todos os recursos e licenças instaladas para implementar detecção de ataques de negação de serviço (Denial of Service - DoS);
1.55 A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização via interface gráfica
1.56 A solução deve permitir a atualização de firmware com agendamentos e individualmente dos pontos de acesso, garantindo a gestão e operação simultânea dos access points;
1.57 O fornecedor da solução deve ser responsável por manter a controladora wireless sempre atualizada, utilizando as recomendações do fabricante e gestor técnico do projeto durante todo o período de contrato;
1.58 A solução deverá permitir a continuidade da operação da rede wireless, mesmo que com recursos limitados, após o encerramento do período contrato, ou deve ser possível converter os pontos de acesso para modelo on-premisse (FIT), onde passam a ser controlados por uma controladora local;

2. ESPECIFCAÇÕES TÉCNICAS – PONTO DE ACESSO SEM FIO INDOOR

2.01 Deve permitir o acesso dos dispositivos à rede através de conexão WiFi e que suporte associação com uma controladora wireless em nuvem e/ou local utilizando protocolo de descoberta que opere nas camadas 2 e 3;
2.02 Deve suportar gerência centralizada através de uma controladora wireless capaz de realizar a gestão dos access points e monitoramento de dispositivos conectados a rede;
2.03 Deve suportar gerenciamento remoto estando ou não associado a controladora wireless;
2.04 Deve suportar conexões de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea;
2.05 Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;
2.06 Deve possuir capacidade de monitorar, identificar e proteger em tempo real a rede contra interferências e ameaças;
2.07 Deve suportar uma faixa mínima entre 250(duzentos e cinquenta) e 512 (quinhentos e doze) clientes wireless simultaneamente;
2.08 Deve possuir no mínimo 1 (uma) interface Ethernet padrão 100/1000Base-T com conector RJ-45;
2.09 Deve possuir acesso para gerenciamento local, no mínimo através do padrão RJ45 Ethernet, ainda que esta seja a interface utilizada para a conectividade com a rede;
2.10 Deve suportar alimentação elétrica através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at;
2.11 Deve suportar a implementação de SSID em modo Bridge Mode e Túnel, também conhecido como Local Switching, respectivamente permitindo que todo o tráfego seja comutado localmente nas interfaces ethernets do access points e do gateway ou encaminhado para a controladora wireless;

2.12 Deve suportar o encaminhamento do tráfego de dados dos clientes wireless através de túnel para um concentrador;
2.13 Deve suportar operação em modo Mesh;
2.14 Deve possuir potência de irradiação mínima de 18dBm em ambas as frequências;
2.15 Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1.2 Gbps em um único rádio;
2.16 Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);
2.17 Deve suportar OFDMA com operações em Downlink (DL) e Uplink (UL);
2.18 Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax;
2.19 Deve suportar recurso de Target Wake Time (TWT);
2.20 Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz;
2.21 Deve possuir antenas internas ou externas, desde que todos os slots de entrada de antenas estejam populados, garantindo a potência E.I.R.P. (Effective Isotropic Radiated Power) com ganho mínimo de 2.6dBi em 2.4GHz e 3.7dBi em 5Ghz;
2.22 Em conjunto com a controladora wireless, deve possuir a capacidade de otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente ajustes de potência, canais, frequência e convergência de dispositivos moveis entre os access points;
2.23 Em conjunto com o controlador wireless, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;
2.24 Deve suportar mecanismos para detecção de pontos de acesso não autorizados, também conhecidos como Rogue Aps;
2.25 Deve suportar no mínimo 14 SSIDs com operação simultânea e configurações distintas de segurança e rede;
2.26 Deve suportar os seguintes métodos de autenticação: WPA (TKIP), WPA2 (AES) e WPA3;
2.27 Deve suportar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
2.28 Deve suportar os seguintes protocolos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP;
2.29 Deve suportar RADIUS Change of Authorization (CoA);
2.30 Deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
2.31 Deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área e execute o roaming;
2.32 Deve suportar 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 das frequências ou dos pontos de acesso que estão mais próximos;
2.33 Deve suportar o padrão IEEE 802.11e;
2.34 O ponto de acesso deve permitir acesso administrativo à sua interface CLI (linha de comando), a qual deve suportar recursos de diagnósticos e debug localmente, mesmo quando gerenciado via controladora wireless;
2.35 Deve suportar consultas via ICMP ou outros protocolos de monitoramento diretamente no ponto de acesso;
2.36 Deve possuir acessórios para fixação em paredes e tetos;
2.37 Deve ser capaz de operar em ambientes com temperaturas entre 0 e 40º C;
2.38 Deve possuir suporte ao sistema antifurto do tipo Kensington Security Lock ou similar;
2.39 Deve possuir no mínimo 1 (um) indicador luminoso (LED) com capacidade de informar status de conectividade das interfaces físicas e do estado operacional do ponto de acesso;
2.40 O ponto de acesso deverá ser compatível e ser gerenciado através do controlador wireless em nuvem deste processo;
2.41 Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste documento deverão ser fornecidos para o pleno funcionamento desta solução de acordo com o tempo de contrato;
2.42 Deve possuir certificado emitido pela Wi-Fi Alliance;

3. ESPECIFCAÇÕES TÉCNICAS – PONTO DE ACESSO SEM FIO OUTDOOR

3.01 Deve permitir o acesso dos dispositivos à rede através de conexão WiFi e que suporte associação com uma controladora wireless em nuvem e/ou local utilizando protocolo de descoberta que opere nas camadas 2 e 3;
3.02 Deve suportar gerência centralizada através de uma controladora wireless capaz de realizar a gestão dos access points e monitoramento de dispositivos conectados a rede;
3.03 Deve suportar gerenciamento remoto estando ou não associado a controladora wireless;
3.04 Deve suportar conexões de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea;
3.05 Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;
3.06 Deve possuir capacidade de monitorar, identificar e proteger em tempo real a rede contra interferências e ameaças;
3.07 Deve suportar no mínimo 500 (quinhentos) clientes wireless simultaneamente;
3.08 Deve possuir no mínimo 1 (uma) interface Ethernet padrão 100/1000Base-T com conector RJ-45;
3.09 Deve possuir acesso para gerenciamento local, no mínimo através do padrão RJ45 Ethernet, ainda que esta seja a interface utilizada para a conectividade com a rede;
3.10 Deve suportar alimentação elétrica através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at;
3.11 Deve suportar a implementação de SSID em modo Bridge Mode e Túnel, também conhecido como Local Switching, respectivamente permitindo que todo o tráfego seja comutado localmente nas interfaces ethernets do access points e do gateway ou encaminhado para a controladora wireless;
3.12 Deve suportar o encaminhamento do tráfego de dados dos clientes wireless através de túnel para um concentrador;
3.13 Deve suportar operação em modo Mesh;
3.14 Deve possuir potência de irradiação mínima entre 18dBm e 20 dBm em ambas as frequências;
3.15 Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1.2 Gbps em um único rádio;
3.16 Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);
3.17 Deve suportar OFDMA com operações em Downlink (DL) e Uplink (UL);
3.18 Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax;
3.19 Deve suportar recurso de Target Wake Time (TWT);
3.20 Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz;
3.21 Deve possuir antenas internas ao equipamento com ganho mínimo de 3dBi em 2.4GHz e 4dBi em 5GHz;
3.22 Em conjunto com a controladora wireless, deve possuir a capacidade de otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente ajustes de potência, canais, frequência e convergência de dispositivos moveis entre os access points;
3.23 Em conjunto com o controlador wireless, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;
3.24 Deve suportar mecanismos para detecção de pontos de acesso não autorizados, também conhecidos como Rogue Aps;
3.25 Deve suportar no mínimo 14 SSIDs com operação simultânea e configurações distintas de segurança e rede;
3.26 Deve suportar os seguintes métodos de autenticação: WPA (TKIP), WPA2 (AES) e WPA3;
3.27 Deve suportar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
3.28 Deve suportar os seguintes protocolos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP;

3.29 Deve suportar RADIUS Change of Authorization (CoA);
3.30 Deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
3.31 Deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área e execute o roaming;
3.32 Deve suportar 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 das frequências ou dos pontos de acesso que estão mais próximos;
3.33 Deve suportar o padrão IEEE 802.11e;
3.34 O ponto de acesso deve permitir acesso administrativo à sua interface CLI (linha de comando), a qual deve suportar recursos de diagnósticos e debug localmente, mesmo quando gerenciado via controladora wireless;
3.35 Deve suportar consultas via ICMP ou outros protocolos de monitoramento diretamente no ponto de acesso;
3.36 Deve possuir acessórios para fixação em paredes e tetos;
3.37 Deve ser capaz de operar em ambientes com temperaturas entre -10 e 60º C;
3.38 Deve possuir grau de proteção IP67 ou IP68. Não serão aceitos equipamentos instalados em acessórios, por exemplo caixas herméticas, para que alcancem este grau de proteção;
3.39 Deve possuir no mínimo 1 (um) indicador luminoso (LED) com capacidade de informar status das de conectividade das interfaces físicas e do estado operacional do ponto de acesso;
3.40 O ponto de acesso deverá ser compatível e ser gerenciado através do controlador wireless em nuvem deste processo;
3.41 Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste documento deverão ser fornecidos para o pleno funcionamento desta solução de acordo com o tempo de contrato;
3.42 Deve possuir certificado Anatel e certificado Wi-Fi Alliance válido na entrega do equipamento;