

**1. ITEM 1 - ACCESS POINT Tipo 1 - PONTO DE ACESSO 802.11ax DUAL-BAND 2x2 OU SUPERIOR 2.4GHz e 5GHz INDOOR COM GARANTIA DE 57 MESES – Administrativo**

**1.1 Especificações gerais**

1.1.1 Todos os equipamentos da infraestrutura de rede sem fio fornecidos - equipamentos, peças e acessórios - devem ser novos e constar na linha de produção do fabricante, sem data de descontinuidade definida na publicação do Edital.

- a. Não serão admitidos produtos reconicionados.
- b. Não serão admitidos produtos cuja compatibilidade não seja homologada pelo fabricante.
- c. A comprovação deste item dar-se-á por carta emitida pelo FABRICANTE ou por documento presente em seu sítio público. Caso o documento esteja em língua estrangeira, far-se-á necessária carta emitida pelo FABRICANTE em língua portuguesa que ratifique os termos do documento público.

1.1.2 Todos os equipamentos da infraestrutura de rede cabeada fornecidos devem vir acompanhados dos manuais e documentação completa para instalação e configuração, mídias, programas, cabos e acessórios de todos os componentes adquiridos.

1.1.3 Deverá ser do mesmo fabricante do controlador WLAN para fins de compatibilidade.

1.1.4 Deverá possuir estrutura que permita a utilização do equipamento em locais internos, com fixação em teto e parede.

1.1.5 Deverá ser apresentado o certificado dentro do prazo de validade referente à homologação da Agência Nacional de Telecomunicações (ANATEL) para o produto, com data anterior à publicação do edital, conforme a resolução 242. Não serão aceitos protocolos de entrada ou outros documentos diferentes do certificado, uma vez que os mesmos não garantem o fornecimento de equipamentos homologados e em conformidade com as leis brasileiras.

1.1.6 Visando a plena compatibilidade do ponto de acesso com o padrão WiFi 6 e suas respectivas funcionalidades, a citar, de forma não-exaustiva, DL OFDMA, UL OFDMA, DL MU-MIMO e se faz necessário que o equipamento ofertado esteja listado como Wi-Fi CERTIFIED 6 pela WiFi Alliance na data do pregão.

1.1.7 Deve ser compatível com o padrão UL 2043, o qual regula os componentes dos materiais com o intuito de proteger contra danos causados por fogo, bem como pela fumaça.

1.1.8 Suportar, no mínimo, 400 (quatrocentos) usuários wireless simultâneos, sem nenhum tipo de licença adicional.

1.1.9 Possuir suporte a pelo menos 16 (dezesseis) SSIDs por ponto de acesso.

1.1.10 Possibilitar alimentação elétrica local via fonte de alimentação com seleção automática de tensão (100-240V) e via padrão PoE (IEEE 802.3at ou 802.3bt). Ademais, para PoE, a alimentação elétrica deve ocorrer através de uma única interface de rede, sem perda de funcionalidade e de desempenho.

1.1.11 Deve suportar temperatura de operação entre 0°C a 50°C.

1.1.12 Não deverá possuir antenas aparentes externas ao ponto de acesso, evitando desta forma que estas sejam removidas, o que ocasionaria a degradação do desempenho da rede sem fio.

1.1.13 Deverá possuir até 2 (duas) interfaces ethernet, sendo que o equipamento deve suportar velocidades de pelo menos 10/100/1000/2500 Mbps, utilizando conector RJ-45, para conexão à rede local.

1.1.14 Deverá possuir, no mínimo, um rádio embarcado para IoT com suporte aos protocolos BLE ou ZigBee.

1.1.15 Deverá possuir de uma porta USB para inserção de módulo IoT compatível com BLE e ZigBee ou possuir hardware BLE e ZigBee interno.

1.1.16 Deverá possuir LEDs para a indicação do status da alimentação do ponto de acesso, rádios de 2.4 GHz e 5 GHz.

1.1.17 Deverá ser fornecido com todas as funcionalidades de segurança, incluindo WIPS/WIDS.

1.1.18 Deve ser compatível com IPv4, IPv6 e dual-stack.

## **1.2 Características dos rádios**

1.2.1 O ponto de acesso deverá atender aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax, com operação nas frequências de 2.4 GHz e 5 GHz de forma simultânea.

1.2.2 Implementar as seguintes taxas de transmissão com fallback automático:

IEEE 802.11b: 1 Mbps a 11 Mbps;

IEEE 802.11a e IEEE 802.11g: 6 Mbps a 54 Mbps;

IEEE 802.11n: 6.5 Mbps a 600 Mbps;

IEEE 802.11ac: 6.5 Mbps a 1732 Mbps;

IEEE 802.11ax: 4 Mbps a 2400 Mbps.

- 1.2.3 Deverá possuir antenas internas e integradas com padrão de irradiação omnidirecional compatíveis com as frequências de rádio dos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax, com ganhos de, no mínimo, 3 dBi para 2.4GHz e 3 dBi para 5GHz.
- 1.2.4 Deverá suportar potência agregada de saída, considerando todas as cadeias MIMO, de, no mínimo, 20 dBm na frequência de 5 GHz e 20 dBm na frequência de 2.4 GHz.
- 1.2.5 Deverá suportar canalização de 20 MHz, 40 MHz, 80 MHz e 160 MHz.
- 1.2.6 Deverá possuir mecanismo de rádio com suporte 2x2 e 2 fluxos espaciais ou superior em 5 GHz e 2.4 GHz para MU-MIMO.
- 1.2.7 Deve possuir sensibilidade mínima de recepção de -90dBm considerando MCS0 HE20 (802.11ax) em 5GHz e -92dBm considerando MCS0 HE20 (802.11ax) em 2.4GHz.
- 1.2.8 Deve permitir ajustes dinâmicos do sinal de rádio frequência para otimizar o tamanho da célula de abrangência do ponto de acesso.
- 1.2.9 Deve possuir capacidade de selecionar automaticamente o canal de transmissão.
- 1.2.10 Deve suportar os padrões IEEE 802.11r, IEEE 802.11k e IEEE 802.11v.

### **1.3 Serviços, segurança e gerenciamento**

- 1.3.1 Deve permitir controle e gerenciamento pelo controlador WLAN através de Camada 2 ou 3 do modelo OSI.
- 1.3.2 Em caso de falha de comunicação entre os pontos de acesso e o controlador WLAN, os usuários associados à rede sem fio devem continuar conectados com acesso à rede. Além disso, deve ser possível que novos usuários se associem à rede sem fio utilizando autenticação do tipo IEEE 802.1x mesmo que os pontos de acesso estejam sem comunicação com a controladora.
- 1.3.3 Deve suportar, somente por meio do ponto de acesso em conjunto com o controlador de rede sem fio, a identificação e controle de aplicações dos dispositivos clientes conectados ao ponto de acesso, levando em consideração a camada 7 do modelo OSI.
- 1.3.4 Deve suportar a configuração de limite de banda por usuário ou por SSID.
- 1.3.5 Deve oferecer suporte a mecanismo de localização e rastreamento de usuários (Location Based Services) ou Asset tracking.
- 1.3.6 Implementar cliente DHCP, para configuração automática de seu endereço IP e implementar também suporte a endereçamento IP estático.

- 1.3.7 Deve suportar VLANs conforme o padrão IEEE 802.1Q.
- 1.3.8 Deve suportar atribuição dinâmica de VLAN por usuário.
- 1.3.9 Deve implementar balanceamento de usuários por ponto de acesso.
- 1.3.10 Deve suportar mecanismo que identifique e associe clientes preferencialmente na banda de 5GHz, deixando a banda de 2.4 GHz livre para dispositivos que trabalhem somente nesta frequência.
- 1.3.11 Deve implementar mecanismo para otimização de roaming entre pontos de acesso.
- 1.3.12 Deve suportar HotSpot 2.0 ou Hotspot WISPr e Captive Portal interno e externo.
- 1.3.13 Implementar, pelo menos, os seguintes padrões de segurança wireless:
- (WPA) Wi-Fi Protected Access;
  - (WPA2) Wi-Fi Protected Access 2;
  - (WPA3) Wi-Fi Protected Access 3;
  - (AES) Advanced Encryption Standard;
  - (TKIP) Temporal Key Integrity Protocol;
  - Deve implementar funcionalidade para geração de chaves compartilhadas dinâmicas de acesso à rede sem fio, como DPSK, MPSK, iPSK, ou similar;
  - IEEE 802.1X;
  - IEEE 802.11i.
- 1.3.14 Deverá permitir a criação de filtros de endereços MAC de forma a restringir o acesso à rede sem fio.
- 1.3.15 Deverá permitir a criação de listas de controle de acesso de Camada 3 e 4 do modelo OSI.
- 1.3.16 Deve permitir habilitar e desabilitar a divulgação do SSID.
- 1.3.17 Deverá implementar autenticação de usuários usando portal de captura.
- 1.3.18 Deve implementar autenticação de usuários usando WISPr ou Hotspot 2.0.
- 1.3.19 Deverá suportar funções para análise de espectro.
- 1.3.20 Deve disponibilizar uma página local acessível pelo cliente conectado ao ponto de acesso para visualização de estatísticas de conexão e informações do respectivo ponto de acesso.
- 1.3.21 Deve suportar conversão de tráfego multicast para unicast.

- 1.3.22 Permitir a configuração e gerenciamento direto através de navegador padrão (HTTPS), SSH, SNMPv2c, SNMPv3 ou através do controlador, a fim de se garantir a segurança dos dados.
- 1.3.23 Permitir que sua configuração seja realizada automaticamente quando este for conectado ao controlador WLAN do mesmo fabricante.
- 1.3.24 Implementar funcionamento em modo gerenciado por controlador WLAN, para configuração de seus parâmetros wireless, das políticas de segurança, QoS, autenticação e monitoramento de RF.
- 1.3.25 Permitir que o processo de atualização de software seja realizado manualmente através de interface Web, FTP ou TFTP e automaticamente através de controlador WLAN do mesmo fabricante.

## **2. ITEM 2 - ACCESS POINT Tipo 2 - PONTO DE ACESSO 802.11ax DUAL-BAND 4x4 2.4GHz e 4x4 5GHz INDOOR COM GARANTIA DE 57 MESES – Auditório**

### **2.1 Especificações gerais**

- 2.1.1 Todos os equipamentos da infraestrutura de rede sem fio fornecidos - equipamentos, peças e acessórios - devem ser novos e constar da linha de produção do fabricante, sem data de descontinuidade definida na publicação do Edital.
  - a. Não serão admitidos produtos reconicionados.
  - b. Não serão admitidos produtos cuja compatibilidade não seja homologada pelo fabricante.
  - c. A comprovação deste item dar-se-á por carta emitida pelo FABRICANTE ou por documento presente em seu sítio público. Caso o documento esteja em língua estrangeira, far-se-á necessária carta emitida pelo FABRICANTE em língua portuguesa que ratifique os termos do documento público.
- 2.1.2 Todos os equipamentos da infraestrutura de rede cabeada fornecidos devem vir acompanhados dos manuais e documentação completa para instalação e configuração, mídias, programas, cabos e acessórios de todos os componentes adquiridos.
- 2.1.3
- 2.1.4 Deverá ser do mesmo fabricante do controlador WLAN para fins de compatibilidade.
- 2.1.5 Deverá possuir estrutura que permita a utilização do equipamento em locais internos, com fixação em teto e parede.
- 2.1.6 Deverá ser apresentado o certificado dentro do prazo de validade referente à homologação da Agência Nacional de Telecomunicações (ANATEL) para o produto, com data anterior à publicação do edital, conforme a resolução 242. Não serão aceitos protocolos de entrada ou outros documentos diferentes do certificado, uma vez que os mesmos não garantem o fornecimento de equipamentos homologados e em conformidade com as leis brasileiras.

- 2.1.7 Visando a plena compatibilidade do ponto de acesso com o padrão WiFi 6 e suas respectivas funcionalidades, a citar, de forma não-exaustiva, DL OFDMA, UL OFDMA, DL MU-MIMO e se faz necessário que o equipamento ofertado esteja listado como Wi-Fi CERTIFIED 6 pela WiFi Alliance na data do pregão.
- 2.1.8 Deve ser compatível com o padrão UL 2043, o qual regula os componentes dos materiais com o intuito de proteger contra danos causados por fogo, bem como pela fumaça.
- 2.1.9 Suportar, no mínimo, 500 (quinhentos) usuários wireless simultâneos, sem nenhum tipo de licença adicional.
- 2.1.10 Possuir suporte a pelo menos 16 (dezesseis) SSIDs por ponto de acesso.
- 2.1.11 Possibilitar alimentação elétrica local via fonte de alimentação com seleção automática de tensão (100-240V) e via padrão PoE (IEEE 802.3at ou 802.3bt). Ademais, para PoE, a alimentação elétrica deve ocorrer através de uma única interface de rede, sem perda de funcionalidade e de desempenho.
- 2.1.12 Deve suportar temperatura de operação entre 0°C a 50°C.
- 2.1.13 Não deverá possuir antenas aparentes externas ao ponto de acesso, evitando desta forma que estas sejam removidas, o que ocasionaria a degradação do desempenho da rede sem fio.
- 2.1.14 Deverá possuir até 2 (duas) interfaces ethernet, sendo que o equipamento deve suportar velocidades de pelo menos 10/100/1000/2500 Mbps, utilizando conector RJ-45, para conexão à rede local.
- 2.1.15 Deverá possuir, no mínimo, um rádio embarcado para IoT com suporte aos protocolos BLE ou ZigBee.
- 2.1.16 Deverá possuir de uma porta USB para inserção de módulo IoT compatível com BLE e ZigBee ou possuir hardware BLE e ZigBee interno.
- 2.1.17 Deverá possuir LEDs para a indicação do status da alimentação do ponto de acesso, rádios de 2.4 GHz e 5 GHz.
- 2.1.18 Deverá ser fornecido com todas as funcionalidades de segurança, incluindo WIPS/WIDS.
- 2.1.19 Deve ser compatível com IPv4, IPv6 e dual-stack.

## **2.2 Características dos rádios**

- 2.2.1 O ponto de acesso deverá atender aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax, com operação nas frequências de 2.4 GHz e 5 GHz de forma simultânea.

2.2.2 Implementar as seguintes taxas de transmissão com fallback automático:

- 2.2.2.1.1 IEEE 802.11b: 1 Mbps a 11 Mbps;
- 2.2.2.1.2 IEEE 802.11a e IEEE 802.11g: 6 Mbps a 54 Mbps;
- 2.2.2.1.3 IEEE 802.11n: 6.5 Mbps a 600 Mbps;
- 2.2.2.1.4 IEEE 802.11ac: 6.5 Mbps a 1732 Mbps;
- 2.2.2.1.5 IEEE 802.11ax: 4 Mbps a 2400 Mbps.

2.2.3 Deverá possuir antenas internas e integradas com padrão de irradiação omnidirecional compatíveis com as frequências de rádio dos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax, com ganhos de, no mínimo, 3 dBi para 2.4GHz e 3 dBi para 5GHz.

2.2.4 Deverá suportar potência agregada de saída, considerando todas as cadeias MIMO, de, no mínimo, 23 dBm na frequência de 5 GHz e 21 dBm na frequência de 2.4 GHz.

2.2.5 Deverá suportar canalização de 20 MHz, 40 MHz, 80 MHz e 160 MHz.

2.2.6 Deverá possuir mecanismo de rádio com suporte 4x4 e 4 fluxos espaciais em 5 GHz e em 2.4 GHz para MU-MIMO.

2.2.7 Deve possuir sensibilidade mínima de recepção de -90dBm considerando MCS0 HE20 (802.11ax) em 5GHz e -92dBm considerando MCS0 HE20 (802.11ax) em 2.4GHz.

2.2.8 Deve permitir ajustes dinâmicos do sinal de rádio frequência para otimizar o tamanho da célula de abrangência do ponto de acesso.

2.2.9 Deve possuir capacidade de selecionar automaticamente o canal de transmissão.

2.2.10 Deve suportar os padrões IEEE 802.11r, IEEE 802.11k e IEEE 802.11v.

## **2.3 Serviços, segurança e gerenciamento**

2.3.1 Deve permitir controle e gerenciamento pelo controlador WLAN através de Camada 2 ou 3 do modelo OSI.

2.3.2 Em caso de falha de comunicação entre os pontos de acesso e o controlador WLAN, os usuários associados à rede sem fio devem continuar conectados com acesso à rede. Além disso, deve ser possível que novos usuários se associem à rede sem fio utilizando autenticação do tipo IEEE 802.1x mesmo que os pontos de acesso estejam sem comunicação com a controladora.

2.3.3 Deve suportar, somente por meio do ponto de acesso em conjunto com o controlador de rede sem fio, a identificação e controle de aplicações dos dispositivos clientes conectados ao ponto de acesso, levando em consideração a camada 7 do modelo OSI.

- 2.3.4 Deve suportar a configuração de limite de banda por usuário ou por SSID.
- 2.3.5 Deve oferecer suporte a mecanismo de localização e rastreamento de usuários (Location Based Services) ou Asset tracking.
- 2.3.6 Implementar cliente DHCP, para configuração automática de seu endereço IP e implementar também suporte a endereçamento IP estático.
- 2.3.7 Deve suportar VLANs conforme o padrão IEEE 802.1Q.
- 2.3.8 Deve suportar atribuição dinâmica de VLAN por usuário.
- 2.3.9 Deve implementar balanceamento de usuários por ponto de acesso.
- 2.3.10 Deve suportar mecanismo que identifique e associe clientes preferencialmente na banda de 5GHz, deixando a banda de 2.4 GHz livre para dispositivos que trabalhem somente nesta frequência.
- 2.3.11 Deve implementar mecanismo para otimização de roaming entre pontos de acesso.
- 2.3.12 Deve suportar HotSpot 2.0 ou Hotspot WISPr e Captive Portal interno e externo.
- 2.3.13 Implementar, pelo menos, os seguintes padrões de segurança wireless:
  - 2.3.13.1 (WPA) Wi-Fi Protected Access;
  - 2.3.13.2 (WPA2) Wi-Fi Protected Access 2;
  - 2.3.13.3 (WPA3) Wi-Fi Protected Access 3;
  - 2.3.13.4 (AES) Advanced Encryption Standard;
  - 2.3.13.5 (TKIP) Temporal Key Integrity Protocol;
  - 2.3.13.6 Deve implementar funcionalidade para geração de chaves compartilhadas dinâmicas de acesso à rede sem fio, como DPSK, MPSK, iPSK, ou similar;
  - 2.3.13.7 IEEE 802.1X;
  - 2.3.13.8 IEEE 802.11i.
- 2.3.14 Deverá permitir a criação de filtros de endereços MAC de forma a restringir o acesso à rede sem fio.
- 2.3.15 Deverá permitir a criação de listas de controle de acesso de Camada 3 e 4 do modelo OSI.
- 2.3.16 Deve permitir habilitar e desabilitar a divulgação do SSID.
- 2.3.17 Deverá implementar autenticação de usuários usando portal de captura.
- 2.3.18 Deve implementar autenticação de usuários usando WISPr ou Hotspot 2.0.



- 2.3.19 Deverá suportar funções para análise de espectro.
- 2.3.20 Deve disponibilizar uma página local acessível pelo cliente conectado ao ponto de acesso para visualização de estatísticas de conexão e informações do respectivo ponto de acesso.
- 2.3.21 Deve suportar conversão de tráfego multicast para unicast.
- 2.3.22 Permitir a configuração e gerenciamento direto através de navegador padrão (HTTPS), SSH, SNMPv2c, SNMPv3 ou através do controlador, a fim de se garantir a segurança dos dados.
- 2.3.23 Permitir que sua configuração seja realizada automaticamente quando este for conectado ao controlador WLAN do mesmo fabricante.
- 2.3.24 Implementar funcionamento em modo gerenciado por controlador WLAN, para configuração de seus parâmetros wireless, das políticas de segurança, QoS, autenticação e monitoramento de RF.
- 2.3.25 Permitir que o processo de atualização de software seja realizado manualmente através de interface Web, FTP ou TFTP e automaticamente através de controlador WLAN do mesmo fabricante.

### **3. ITEM3 - CONTROLADORA WIRELESS - WLAN CONTROLLER - COM GARANTIA DE 57 MESES**

#### **3.1. GERAL**

3.1.1. Todos os equipamentos da infraestrutura de rede sem fio fornecidos - equipamentos, peças e acessórios - devem ser novos e constar na linha de produção do fabricante, sem data de descontinuidade definida na publicação do Edital.

- a. Não serão admitidos produtos recondicionados.
- b. Não serão admitidos produtos cuja compatibilidade não seja homologada pelo fabricante.
- c. A comprovação deste item dar-se-á por carta emitida pelo FABRICANTE ou por documento presente em seu sítio público. Caso o documento esteja em língua estrangeira, far-se-á necessária carta emitida pelo FABRICANTE em língua portuguesa que ratifique os termos do documento público.

3.1.2. Todos os equipamentos da infraestrutura de rede cabeada fornecidos devem vir acompanhados dos manuais e documentação completa para instalação e configuração, mídias, programas, cabos e acessórios de todos os componentes adquiridos.

3.1.3. O controlador WLAN poderá ser do tipo virtual e compatível com os ambientes VMWare 7.0 e superiores, Hyper-V Windows 2019 e 2022. O ambiente virtualizado deverá ser disponibilizado em servidor ou servidores da CONTRATANTE com as especificações recomendadas pelo fabricante da solução; O fornecedor poderá fornecer também a opção em appliance físico que deverá ter pelo menos 4 portas 10G SFP+, o qual deve estar populado com os respectivos módulos.

3.1.4. Não serão aceitas soluções baseadas nas premissas de computação em nuvem, pontos de acesso autônomos ou controladores agregados a outros equipamentos, tais como Switches, Firewalls, Roteadores ou até mesmo controlador virtual dentro do próprio ponto de acesso;

3.1.5. Não serão aceitos sistemas implementados em virtualizadores de desktop, tais como Oracle VM VirtualBox ou VMware Workspace;

3.1.6. Deverá ser do mesmo fabricante dos pontos de acesso fornecidos pela CONTRATADA, para fins de compatibilidade e gerenciamento;

3.1.7. Deverá suportar operação como um cluster (N+1) para prover resiliência e desempenho.

3.1.8. Deve vir acompanhado de todos os acessórios necessários para operacionalização da solução, tais como softwares, documentações técnicas e manuais que contenham informações suficientes, que possibilitem a instalação, configuração e operacionalização da solução;

3.1.9. Deve possuir uma arquitetura modular, permitindo gestão centralizada.

3.1.10. Deverá suportar pontos de acesso internos e externos nos padrões 802.11a/b/g/n/ac/ax;

3.1.11. Deverá possuir suporte a RESTful API compatível com JSON e disponibilizar suporte às funções GET, POST, DELETE, PUT e PATCH;

## **3.2. GERENCIAMENTO**

3.2.1. Capacidade para gerenciar, no mínimo, 300 (trezentos) Pontos de Acesso, podendo chegar através de atualização de licenças de software a até 4800 (quatro mil e oitocentos) Pontos de Acesso simultâneos por controlador;

3.2.2. Suportar, no mínimo, 10000 (dez mil) dispositivos simultâneos por controlador;

3.2.3. Prover o gerenciamento centralizado dos Pontos de Acesso, suportando versões de firmware diferentes;

3.2.4. Deverá permitir gerenciamento através de Endereço IP, Range de IPs e Sub-Redes pré-configuradas;

3.2.5. Permitir a configuração total dos pontos de acesso, assim como os aspectos de segurança da rede wireless (WLAN) e Rádio Frequência (RF);

3.2.6. O controlador WLAN poderá estar diretamente e/ou remotamente conectado aos Pontos de Acesso por ele gerenciados, inclusive via roteamento em camada 3 do modelo OSI;

3.2.7. Possibilitar a configuração de envio dos eventos do Controlador WLAN para um servidor de Syslog remoto;

3.2.8. Implementar, pelo menos, os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps SNMP;

3.2.9. Permitir a visualização de alertas da rede em tempo real;

3.2.10. Implementar, no mínimo, 3 (três) níveis de acesso administrativo ao equipamento (apenas leitura, leitura/escrita e administrador da senha de visitante) protegidos por senhas independentes;

3.2.11. Permitir a customização do acesso administrativo através de atribuição de grupo de função do usuário administrador;

3.2.12. Permitir a configuração de servidores AAA para autenticação dos usuários administrativos;

3.2.13. Deve ser possível definir o nível de segurança administrativo da solução suportando, no mínimo:

3.2.13.1. Período em dias para alteração obrigatória da senha;

3.2.13.2. Política para reutilização de senha;

3.2.13.3. Comprimento mínimo da senha e complexidade;

3.2.14. Permitir a configuração e gerenciamento através de navegador padrão por meio de HTTPS;

3.2.15. Gerenciar de forma centralizada a autenticação de usuários administradores e clientes da rede sem fio;

3.2.16. Permitir o envio de alertas ou alarmes através do protocolo SMTP, sendo que a comunicação com o servidor deverá ser autenticada e cifrada (SMTP/TLS);

3.2.17. Permitir que o processo de atualização de versão seja realizado através de navegador padrão (HTTPS) ou SSH;

3.2.18. Permitir o agendamento da atualização de firmware dos pontos de acesso gerenciais por zona ou por grupo;

3.2.19. Deverá possuir a capacidade de importação de certificados digitais emitidos por uma autoridade certificadora externa.;

3.2.20. A disponibilidade da rede sem fio deve ser passível de agendamento para, no mínimo, as opções a seguir:

3.2.20.1. 24 horas por dia, 7 dias na semana;

3.2.20.2. Agendamento customizado permitindo escolher os dias da semana e horários;

3.2.20.3. Os horários definidos não precisam ser sequenciais, ou seja, a solução deve suportar que o administrador defina o horário de funcionamento das 08:00 às 12:00 e 14:00 às 18:00;

3.2.21. Possuir ferramentas de diagnóstico e log de eventos para depuração e gerenciamento em primeiro nível;

3.2.22. Possuir ferramenta que permite o monitoramento em tempo real de informações de utilização de CPU, memória e estatísticas de rede;

3.2.23. Possibilitar cópia “backup” da configuração, bem como a funcionalidade de restauração da configuração através de navegador padrão (HTTPS) ou FTP ou TFTP;

3.2.24. Possuir a capacidade de armazenar múltiplos arquivos de configuração do controlador pertencente à rede sem fio;

3.2.25. Monitorar o desempenho da rede sem fio, permitindo a visualização de informações gerais e de cada ponto de acesso;

3.2.26. Implementar cluster de controladores WLAN no modo ativo/ativo ou ativo/standby, com sincronismo automático das configurações entre controladores para suporte a redundância em alta disponibilidade (HA - high availability);

3.2.26.1. Deverá efetuar compartilhamento de recursos e licenças de pontos de acesso entre os controladores participantes do cluster;

3.2.26.2. Deverá, em caso de falha, realizar a redundância de forma automática e sem nenhuma necessidade de intervenção do administrador de rede;

3.2.26.3. Deve manter as conexões wireless dos usuários já associados, caso um dos elementos do cluster venha a sofrer queda de rede (ativo/ativo) ou no caso ativo/standby quando o ativo sofrer uma queda de rede. Além disso, deve aceitar novas conexões durante o período de queda.

3.2.27. Deverá possuir a capacidade de geração de informações ou relatórios de, no mínimo, os seguintes tipos: Listagem de clientes Wireless, Listagem de Pontos de Acesso, utilização da rede;

3.2.28. Deverá suportar, somente por meio do controlador e do ponto de acesso, a identificação de aplicações dos dispositivos clientes conectados aos pontos de acesso com base na camada 7 do modelo OSI, permitindo o controle de acesso, de banda (uplink e/ou downlink) e definição de regra de QoS para estas aplicações;

3.2.28.1. Deve permitir a atualização do pacote de assinaturas para identificação das aplicações utilizadas pelos dispositivos clientes conectados aos pontos de acesso;

3.2.29. Deve ser possível especificar regras de usuários baseadas em tempo, permitindo determinar em quais dias e horários a regra estará ativa, possibilitando ainda que os horários não sejam obrigatoriamente sequenciais, ou seja, deve ser possível escolher das 08:00 às 12:00 e das 14:00 às 18:00, por exemplo;

3.2.30. Permitir visualizar a localização dos pontos de acesso e através desta obter o seu estado de funcionamento;

3.2.31. Deverá possibilitar a importação de plantas baixas nos formatos dwg ou jpg ou png, devendo permitir a visualização dos Pontos de Acesso instalados com seu estado de funcionamento, bem como disponibilizar uma visualização da cobertura do sinal em 2.4GHz ou 5GHz;

3.2.32. Deve ser possível localizar o access point na planta baixa;

3.2.33. Implementar funcionalidade de análise espectral em tempo real e por frequência, 2.4GHz ou 5GHz permitindo a detecção de interferências e geração de gráficos de uso do ambiente de rede sem fio;

3.2.34. Implementar análise de tráfego por WLAN, Ponto de acesso e dispositivos cliente, apresentando os 10 itens mais usados;

3.2.35. Deve suportar integração com tags da Ekahau e/ou AeroScout/Stanley para Real-Time Location Service (RTLS);

3.2.36. O tráfego do wlan visitante deve passar pela controladora.

### **3.3. REDE**

3.3.1. Deverá implementar suporte aos protocolos IPv4 e IPv6;

3.3.2. Deverá suportar tagging de VLANs;

3.3.3. Implementar associação dinâmica de usuário a VLAN com base nos parâmetros da etapa de autenticação via IEEE 802.1X;

3.3.4. Suportar associação dinâmica de ACL e de QoS por usuário, com base nos parâmetros da etapa de autenticação;

3.3.5. Deverá suportar, no mínimo, 1030 (mil e trinta) SSIDs simultâneos;

3.3.6. Deverá possuir funcionalidade de balanceamento de carga entre VLANs e permitir que clientes sejam designados para diferentes VLANs dentro de um mesmo SSID, com suporte a até 50 VLANs por pool;

3.3.7. Em caso de falha de comunicação entre os pontos de acesso e a controladora, os usuários associados à rede sem fio devem continuar conectados e com acesso à rede. Também deve permitir que novos usuários se associem à rede sem fio utilizando autenticação do tipo 802.1X mesmo que os pontos de acesso estejam sem comunicação com a controladora;

3.3.8. Deve ser possível desabilitar o suporte ao padrão IEEE 802.11b visando aprimorar o desempenho da rede sem fio;

3.3.9. Deve suportar 802.11k;

3.3.10. Deve suportar captura de pacotes por ponto de acesso para resolução de problemas, sendo possível definir a captura nos rádios de 2.4 GHz e 5 GHz, bem como na interface LAN. A operação de captura deve ser realizada via interface Web com a possibilidade de exportação do arquivo de captura para análise local em software específico para análise de pacotes;

3.3.11. Deve ser possível monitorar o processo de conexão de um dispositivo cliente em tempo real com a finalidade de identificar problemas de conectividade e determinar em qual estágio o problema aconteceu;

3.3.12. Deve ser possível estabelecer um limite para o nível de sinal visando permitir que o cliente se junte à rede sem fio, o qual deve ser estabelecido em dBm e variar entre -60dBm e -90dBm;

3.3.13. Deverá suportar de forma centralizada a configuração de agregação de portas (LACP) ethernet dos pontos de acesso que possuírem suporte a essa funcionalidade;

### **3.4. SEGURANÇA**

3.4.1. Os itens a seguir devem estar integrados a solução ofertada, não serão aceitos equipamentos externos a solução para seu atendimento. Caso sejam necessárias licenças ou softwares de controle, os mesmos devem ser fornecidos de forma que a solução esteja operacional e sem nenhuma restrição no ato de sua implementação (hardware e softwares necessários para implementação);

3.4.2. Implementar, pelo menos, os seguintes padrões de segurança wireless:

3.4.2.1. (WPA) Wi-Fi Protected Access;

3.4.2.2. (WPA2) Wi-Fi Protected Access 2;

3.4.2.3. (WPA3) Wi-Fi Protected Access 3;

3.4.2.4. (TKIP) Temporal Key Integrity Protocol;

3.4.2.5. (AES) Advanced Encryption Standard;

3.4.2.6. PSK (Pre-Shared Key) única por dispositivo cliente em um mesmo SSID;

3.4.2.7. IEEE 802.1X;

3.4.2.8. IEEE 802.11i;

3.4.2.9. IEEE 802.11w;

3.4.3. Implementar, pelo menos, os seguintes controles/filtros:

3.4.3.1. Baseado em endereço MAC e isolamento de cliente na camada 2 do modelo OSI;

3.4.3.2. Baseado em endereço IP;

3.4.3.3. Baseado em protocolo, tais como TCP, UDP, ICMP e IGMP;

3.4.3.4. Baseado em porta de origem e/ou destino;

3.4.3.5. Baseado em tipo ou sistema operacional do dispositivo;

3.4.4. Permitir a autenticação para acesso dos usuários conectados nas redes WLAN (Wireless) através:

3.4.4.1. Endereço MAC;

3.4.4.2. Autenticação Local;

3.4.4.3. Captive Portal;

3.4.4.4. Active Directory;

3.4.4.5. RADIUS;

3.4.4.6. IEEE 802.1X;

3.4.4.7. LDAP;

3.4.5. Deverá permitir a seleção/uso de servidor RADIUS específico com base no SSID;

3.4.6. Deverá suportar servidor de autenticação RADIUS redundante. Isto é na falha de comunicação com o servidor RADIUS principal, o sistema deverá buscar um servidor RADIUS secundário;

3.4.7. A solução deverá suportar a criação de uma zona de visitantes, que terá seu acesso controlado através de senha cadastrada internamente, sendo que esta deverá possuir a configuração de tempo pré-determinado de acesso à rede sem fio;

3.4.8. O controlador deverá permitir a criação de múltiplos usuários visitantes (guests) de uma única vez (em lote), podendo ser via software externo;

3.4.9. Deve ser possível definir o período de validade da senha de visitantes em quantidade de horas, dias e semanas;

3.4.10. Deve permitir que após o processo de autenticação de usuários visitantes (guests), os mesmos sejam redirecionados para uma página de navegação específica e configurável;

3.4.11. Deve permitir que múltiplos usuários visitantes (guests) compartilhem a mesma senha de acesso à rede;

3.4.12. Deverá dispor de opção para enviar a senha de usuários visitantes (guests) por e-mail ou por SMS, podendo ser via software externo;

3.4.13. Deve disponibilizar autenticação dos usuários por meio de Redes, suportando, no mínimo, 2 (duas) redes sociais diferentes dentro de uma mesma WLAN.

3.4.14. Deverá permitir o isolamento do tráfego unicast, multicast ou ambos entre usuários visitantes (guests) em uma mesma VLAN/Subrede, sendo possível adicionar exceções com base em endereços MAC e IP;

3.4.15. Deverá permitir o encaminhamento do tráfego de saída de usuários visitantes (guests) diretamente para a Internet, de forma totalmente separada do tráfego da rede corporativa através de VLAN definida na WLAN visitante;

3.4.16. Deverá ser possível permitir que o ponto de acesso filtre todo o tráfego IPv4 e IPv6 dos tipos multicast e broadcast dos clientes sem fio associados, com exceção de alguns tráfegos pertencentes a uma lista de exclusões, tais como ARP, DHCPv4 e DHCPv6, MLD, IGMP, IPv6 NS, IPv6 NA, IPv6 RS e todos os pacotes do tipo unicast;

3.4.17. Deverá ser possível especificar o tipo de serviço Bonjour que será permitido entre VLANs por meio de execução de gateway bonjour nos pontos de acesso;

3.4.18. Deve suportar mecanismo de acesso de acordo com o padrão Hotspot 2.0;

3.4.19. Deve implementar mecanismos de segurança e proteção da rede sem fio contemplando, no mínimo, os recursos abaixo:

3.4.19.1. SSID Spoofing – Detectar APs não pertencentes ao controlador propagando o mesmo SSID;

3.4.19.2. MAC Spoofing – Detectar APs que não pertencem ao controlador e que estejam propagando o mesmo MAC de um AP válido;

3.4.19.3. Rogue APs – Detectar APs não pertencentes ao controlador;

3.4.19.4. Same Network – Detectar APs não pertencentes ao controlador exibindo qualquer SSID pertencentes ao mesmo segmento de rede LAN.;

3.4.19.5. Ad Hoc – Possibilidade de detectar rede Ad Hoc como rogue AP;

3.4.19.6. Flood de Deauthentication – Detectar quando há um número excessivo de frames de desautenticação oriundos de um mesmo transmissor;

3.4.19.7. Flood de Disassociation – Detectar quando há um número excessivo de frames de desassociação oriundos de um mesmo transmissor;

3.4.19.8. Excesso de Clear to Send (CTS) – Detectar quando há um número excessivo de frames de CTS para um endereço MAC específico;

3.4.19.9. Excesso de Request to Send (RTS) – Detectar quando há um número excessivo de frames de RTS para um endereço MAC específico;

3.4.19.10. Excesso de Energia – Possibilidade de detectar tráfego com nível de potência de transmissão excessivo;

3.4.20. Deve implementar varredura de rádio frequência para identificação de ataques e Pontos de Acesso intrusos não autorizados (rogue AP);

3.4.21. Deve fazer a varredura no canal de operação do Ponto de Acesso sem impacto na performance da rede WLAN;

3.4.22. Deve utilizar os Pontos de Acesso para fazer a monitoração do ambiente Wireless procurando por pontos de acesso do tipo rogue de forma automática;

3.4.23. Deve ser possível especificar um ponto de acesso ou grupo de pontos de acesso para atuarem somente com a função de monitoramento visando detectar ataques e analisar o ambiente de rádio frequência;

3.4.24. Deverá ser capaz de localizar Pontos de Acesso do tipo rogue na planta baixa adicionada ao sistema ou graficamente com informações de, no mínimo:



3.4.24.1. Pontos de Acesso que detectam;

3.4.24.2. Tipo de Rogue;

3.4.24.3. Nome da Rede;

3.4.24.4. Nível de sinal de detecção;

### **3.5. RECURSOS DE GERENCIAMENTO AUTOMÁTICO DE RÁDIO FREQUÊNCIA (RF)**

3.5.1. Na ocorrência de inoperância de um Ponto de Acesso, o controlador sem fio deverá ajustar automaticamente a potência dos Pontos de Acesso adjacentes, de modo a prover a cobertura da área não assistida;

3.5.2. Ajustar automaticamente a utilização de canais de modo a otimizar a cobertura de rede e mudar as condições de rádio frequência baseado em desempenho;

3.5.3. Detectar interferência e ajustar parâmetros de rádio frequência, evitando problemas de cobertura de RF de forma automática;

3.5.4. Implementar sistema automático de balanceamento de carga para associação de clientes entre Pontos de Acesso próximos para otimizar o desempenho;

3.5.5. Implementar funcionalidade de balanceamento de carga entre os rádios de um mesmo Ponto de Acesso;

3.5.6. Permitir que o serviço wireless seja desabilitado de determinado ponto de acesso. Também deve ser possível selecionar o serviço de qual rádio (banda) de determinado ponto de acesso deve ser desabilitado;

### **3.6. RECURSOS DE CONVERGÊNCIA E MULTIMÍDIA**

3.6.1. Suportar 802.11e;

3.6.2. Deverá possuir funcionalidade de configuração do limite de banda disponível por usuário ou através de SSID/BSSID;

3.6.3. Deverá permitir a configuração de prioridade de um determinado SSID sobre outros SSIDs existentes na controladora;

3.6.4. Deve suportar WiFi Calling;

## **4. ITEM 4. LICENÇA PARA ACCESS POINT**

4.1. Fornecimento, e garantia de licenças para gerenciamento de Access Point na controladora WLAN e Software de Gerenciamento, caso não estejam incluídos no licenciamento do fabricante;

4.2. Todas as licenças devem ser vitalícias;

4.3. Todas as licenças devem ser instaladas e configuradas sem qualquer ônus adicional.

## 5. ITEM 5 - SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO

5.1. O serviço de instalação e configuração contempla configurar as controladoras em modo cluster e a configuração de 1 Access Point pela CONTRATADA.

5.2. A CONTRATADA deverá instalar, configurar, interconectar, testar e documentar a solução.

5.3. Caberá a CONTRATADA incluir a apresentação do projeto conceitual, cronograma com fases de execução e testes da solução.

5.4. Caberá à CONTRATADA a instalação lógica e física (caso seja fornecido appliance) dos equipamentos, incluindo todos os componentes necessários para o perfeito funcionamento da solução integrada com o parque computacional já existente.

5.5. A instalação compreende, no mínimo:

- a. A desembalagem e montagem de todos os componentes que integram a solução. (caso seja fornecido appliance)
- b. A instalação e energização dos equipamentos montados em rack padrão do CONTRATANTE. (caso seja fornecido appliance)
- c. A instalação dos softwares necessários para o funcionamento da solução.
- d. Os equipamentos deverão ser adequados à estrutura elétrica no Data Center. (caso seja fornecido appliance)

5.6. A configuração compreende, no mínimo:

- a. A realização dos ajustes de hardware (caso seja fornecido appliance) e software necessários ao funcionamento integrado da solução.
- b. Todas as atualizações de firmware ou qualquer outro software componente da solução para a versão mais atualizada disponível ou a última compatível e considerada estável.
- c. Habilitação de licenças, que porventura sejam adquiridas, e recursos dos equipamentos.

5.7. A integração compreende, no mínimo:

- a. As verificações dos recursos e o seu perfeito funcionamento e integração com os demais, conforme as melhores práticas indicadas pelo fabricante.
- b. A interconexão dos equipamentos à rede Ethernet do CONTRATANTE. (caso seja fornecido appliance)
- c. O cluster das controladoras deve ser configurado para seu perfeito funcionamento, caso uma das controladoras fique indisponível, a outra deve assumir e manter as conexões dos clientes wireless já associados antes do incidente, além de aceitar novas requisições de conexão.
- d. O cluster das controladoras deve comunicar perfeitamente com os pontos de acesso locais e remotos.

5.8. Para todos os efeitos, a conclusão do serviço será dada pela entrega da solução em pleno funcionamento, conforme avaliado pela equipe técnica do Tribunal.

5.9. A CONTRATADA deverá cumprir os prazos descritos abaixo, os quais poderão ser antecipados, se assim for possível e acordado com o Tribunal.

ETAPA	PRAZO MÁXIMO (dias corridos)	EVENTO	RESPONSÁVEL
-------	---------------------------------	--------	-------------

Dia D	-	Recebimento da nota de empenho e/ou assinatura do contrato.	Tribunal e CONTRATADA
D1	D + 07	Reunião de KICK-OFF.	Tribunal e CONTRATADA
D2	D1 + 15	Elaboração e apresentação do PROJETO EXECUTIVO da instalação e configuração da solução.	CONTRATADA
D3	D2 + 07	Análise e aprovação técnica do PROJETO EXECUTIVO.	Tribunal
D4	D + 90	Entrega dos equipamentos, softwares e serviços	CONTRATADA
D5	D4 + 10	Recebimento Provisório, conforme cada entrega	Tribunal
D6	Entrega + 30	Instalação e configuração da solução.	CONTRATADA
D7	Conforme recebimentos	Emissão do Termo de Recebimento Definitivo.	Tribunal
D8	D4 + 57 meses	Início da contagem do prazo de garantia	CONTRATADA

5.10. Caberá a CONTRATADA fornecer suporte técnico desde a fase inicial de execução até 03 (três) dias úteis após a entrega do serviço.

5.11. Caberá a CONTRATADA incluir ao final do serviço entrega da documentação completa da nova solução, planilha com Part Numbers, período de garantia, telefones para contato, senhas de acesso, versões de softwares básicos, etc.

## 6. ITEM6 – SERVIÇO DE TRANSFERÊNCIA DE CONHECIMENTO

6.1 O serviço de instalação e configuração da solução ficará a cargo da CONTRATADA e deverá ser na modalidade hands on, procedendo a passagem de conhecimento relativo a tecnologia durante a própria configuração da solução.

6.2 Ficará a cargo da CONTRATADA, após a implantação da solução em pleno funcionamento, a realização de transferência de conhecimento com duração de, no mínimo, 20 (vinte) horas, para que a documentação do projeto seja repassada e o conhecimento disseminado para a equipe do Tribunal pertinente. O repasse do conhecimento será para 06 (seis) pessoas.

6.3 A transferência do conhecimento deverá ser realizada num período, manhã ou tarde, com carga horária diária de 4 horas.

6.4 O repasse de conhecimento deverá incluir informações sobre o procedimento para a implantação das funcionalidades, no projeto específico, bem como o procedimento de alteração, manutenção e operação, incluindo, no mínimo:

- a. Instalação e configuração, utilizando linha de comando e interface gráfica.
- b. Comandos operacionais, utilizando linha de comando e interface gráfica.
- c. Configurações realizadas a fim de interoperabilidade com o parque computacional existente.
- d. Gerência SNMP;
- e. Configuração Radius.
- f. Configuração de WLAN.
- g. Configuração relacionadas a rede de visitantes.
- h. Criação de vlans.
- i. Registro de APs na controladora.
- j. Gerenciamento do cluster na controladora.
- k. Outros recursos proprietários que possam ser utilizados para o monitoramento e Troubleshooting dos equipamentos das localidades.

6.5 O instrutor deverá possuir certificação na solução ofertada.

6.6 Deverá ser emitido certificado para cada aluno contento nome do aluno, CPF, carga horária, dia de início e fim, conteúdo programático.