Anexo I – Requisitos técnicos da Solução

1. Características comuns a todos os itens de fornecimento

1.1 Todos os equipamentos devem ser novos e de primeiro uso, de modelo em linha de produção e sem anúncio ou previsão de encerramento da produção na data da entrega das propostas.

1.2 Não serão aceitos equipamentos remanufaturados (*refurbished*).

1.3 Todos os equipamentos deverão ser acompanhados de todos os componentes e acessórios necessários à sua instalação e funcionamento, o que inclui, eventualmente, cabos e/ou fontes de alimentação, suportes e parafusos.

1.4 Todos os equipamentos deverão ser entregues em caixas originais do fabricante, lacradas e íntegras, sem sinais de rasgos, amassados ou outras imperfeições que possam denotar comprometimento do conteúdo.

1.5 Todos os equipamentos a serem fornecidos terão que ter certificado de homologação válido pela ANATEL na data da entrega das propostas e tais certificados devem estar disponíveis para consulta eletrônica on-line e o caminho para acesso a eles deve ser fornecido pelo proponente.

1.6 Todas as unidades de equipamentos do mesmo item devem ser do mesmo modelo, contando com a mesma revisão de hardware e software e sendo identificados pelo mesmo código junto ao fabricante (Part Number) e ser fornecidos com a versão mais recente do software interno (firmware) disponível na data da entrega.

1.7 No caso de itens que venham ser fornecidos como dispositivos físicos do tipo hardware appliances, excetuando os Pontos de Acesso, deverão suportar operar em faixas de temperatura de 0°C a 45°C, ser acompanhados de fonte de alimentação com seleção automática de tensão (100-240 VAC), LEDs para a indicação do status das portas e atividade, e todos os acessórios e componentes necessários à sua instalação em rack de 19", além de 1 porta de console física para gerenciamento via linha de comando (CLI – Command Line Interface) com conector RS232, RJ-45 ou USB com seu respectivo cabo.

1.8 No caso de itens que venham ser fornecidos como dispositivos físicos do tipo hardware appliances, devem permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação. Devem, ainda, ser entregues em configurações de CPU e memória suficiente e adequada para a execução simultânea de todas as funcionalidades exigidas para o equipamento em questão.

1.9 No caso de itens que venham ser fornecidos como dispositivos virtualizados do tipo virtual appliances, estes deverão ser este compatíveis e homologados para operação com servidores de virtualização VMware ESXi 6 ou superior, KVM ou Microsoft Hyper-V, haja vista que a infraestrutura de virtualização utilizada será a do órgão contratante. Caso seja necessária alguma licença adicional, esta deverá ser

fornecida juntamente com a solução, com a mesma garantia, suporte e o mesmo prazo de vigência da solução que suporta.

1.10 Todas as unidades de todos os itens, equipamentos e softwares aplicativos, deverão ser fabricados pelo mesmo fornecedor, salvo quando explicitamente admitida exceção, e deverão vir acompanhados de toda a documentação necessária ao seu funcionamento e operação. Esta documentação pode ser impressa ou eletrônica/digital, neste último caso devendo ser fornecida gravada em mídia eletrônica a ser entregue juntamente com os itens a que se refere ou, ainda, no caso de estar disponível on-line, ter seu caminho de acesso (atalho/link) fornecido em documento que acompanhe o item a que se refere.

1.11 Deverão ser fornecidas quaisquer outras licenças necessárias ao perfeito funcionamento da solução em atendimento aos requisitos deste documento, e deverá ser acompanhado de todos os itens necessários para operacionalização, tais como sistemas operacionais, softwares de apoio e licenças de software.

1.12 **Todos os itens devem ser fornecidos de forma que possam ser instalados e executados nas dependências do contratante (on premises)**, mesmo na eventual ausência de conexão com a internet. Não serão aceitos itens cujas soluções sejam baseadas em nuvem do fabricante (Software as a Service - SaaS ou Network as a Service – NaaS) ou que tenham modelo de fornecimento como serviço por assinatura (subscription).

1.13 Todos os itens deverão contar com garantia de funcionamento e suporte técnico pelo período mínimo de 60 meses.

1.14 Todos os itens de software devem ser entregues com licenças de uso perpétuo.

1.15 A comprovação de atendimento aos requisitos técnicos aqui presentes deverá ser explícita e apresentada na forma de tabela onde constam as informações a seguir: número do item de requisito técnico, confirmação de atendimento (Sim ou Não), descrição do requisito técnico, referência (com endereço eletrônico/link de acesso) de comprovação de atendimento pelo fabricante e observações (campo livre para informações adicionais). Será fornecida planilha com modelo padrão a ser adotado.

2. Pontos de Acesso (*Access Points*) – características comuns a todos os modelos

2.1 O equipamento deve ser do tipo Ponto de Acesso (*Access Point* ou AP) e vir acompanhado de estrutura que permita fixação em superfícies sólidas na horizontal (teto/forro) e suportar sua eventual instalação na vertical (paredes ou similares) de ambientes internos mediante uso de estruturas de fixação próprias para este fim.

2.2 Deverá suportar operar na faixa de temperaturas de 5 a 40°C e umidade de até 90% (não condensada).

2.3 Possuir luz/luzes (LED) capazes de indicar os status de ligado, conectado à LAN e de atividade de rede WLAN.

2.4 Vir acompanhado de fonte de alimentação DC externa, para alimentação elétrica, com entrada AC bivolt automática (100-240V). Caso não haja possibilidade de fornecimento do item com fonte de alimentação externa, será aceito em substituição e sem custo adicional, que seja acompanhado de adaptador de energia PoE nos padrões descritos no item 5 deste documento.

2.5 Suportar alimentação pelo padrão Power over Ethernet (PoE) IEEE 802.3af ou 802.3at por meio de pelo menos uma das interfaces de rede, de forma que essa alimentação seja suficiente para o pleno funcionamento de todas as características do equipamento sem nenhuma perda de desempenho ou funcionalidades.

2.6 Possuir pelo menos 2 rádios independentes que possam operar simultaneamente nas frequências de 2.4 e 5 GHz e compatibilidade de transmissão e recepção segundo os padrões IEEE 802.11 a/b/g/n/ac/ax (em suas respectivas frequências de operação).

2.7 Todas as antenas devem ser integradas e internas ao equipamento.

2.8 Possuir configuração com memória e CPU dimensionados de forma a permitir a utilização simultânea e constante de todas as características descritas neste item.

2.9 Possuir suporte para instalação de dispositivo antifurto.

2.10 Implementar a tecnologia Wi-Fi 6 (802.11ax) e permitir conectar simultaneamente dispositivos que se comuniquem em qualquer dos padrões tecnológicos anteriores (compatibilidade retroativa): IEEE 802.11: b, g, a, n, ac.

2.11 O modelo ofertado deve possuir Certificado de Conformidade Técnica de produto do tipo Transceptor de Radiação Restrita homologado pela ANATEL, com vigência válida pelo menos até a data do certame.

2.12 O modelo ofertado deve estar, na data da apresentação das propostas, certificado pela Wi-Fi Alliance na categoria Routers, subcategoria "Enterprise/Service Provider Acess Point, Switch/Controller or Router" e, no sumário de certificações, apresentar as certificações:

2.12.1.1 2.4 GHz Spectrum Capabilities
2.12.1.2 5 GHz Spectrum Capabilities
2.12.1.3 Wi-Fi Certified a, b, g, n, ac, 6
2.12.1.4 WMM
2.12.1.5 WPA 3 Enterprise, Personal

2.12.1.6 WPA 2 Enterprise, Personal
2.12.1.7 Protected Management Frames

2.13 Possuir antenas com padrão de radiação omnidirecional, alcançar potência máxima de transmissão de, pelo menos, 21dBm em cada frequência (2,4 GHz e 5 GHz) (podendo ser combinada com o ganho da antena), e sensibilidade mínima de recepção de -92 dBm.

2.14 Operar em canais de 20MHz para os padrões IEEE 802.11a/b/g, 20/40MHz para o padrão IEEE 802.11n e 20/40/80MHz para os padrões IEEE 802.11ac/ax.

2.15 Deve possuir pelo menos 2 interfaces Gigabit Ethernet ou 1 interface Mutigigabit Ethernet, ou uma combinação destas, todas com conectores RJ-45.

2.16 Ser capaz de suportar pelo menos 512 conexões simultâneas de dispositivos clientes associados por Ponto de Acesso e não deve possuir restrição por software ou licença para a quantidade de usuários internos conectados simultaneamente.

2.17 Implementar, suportar ou ser compatível com as seguintes especificações da família de protocolos IEEE 802.11: a, b, g, n, ac, ax, d, h, i, k, v, r, w.

2.18 Suportar operar em modo gerenciado por Controladora WLAN ou independente dela (autogerenciado), e poder ter todas suas características de funcionamento configuradas remotamente pela Controladora WLAN ou diretamente no próprio equipamento por meio de interface de navegador Web padrão HTTP/HTTPS.

2.19 Deve ser capaz de se conectar à Controladora que o gerencia, diretamente ou remotamente via roteamento de camada 3, com tráfego de gerenciamento protegido por túnel criptografado (IEEE 802.11w, Protected Management Frames).

2.20 Implementar seleção automática de canal e ajuste automático de potência do sinal, visando o melhor desempenho.

2.21 Ser capaz de prover 16 SSIDs simultâneos por Ponto de Acesso.

2.22 Permitir escolher entre habilitar e desabilitar a divulgação de qualquer SSID.

2.23 Deve permitir implementar pelo menos 8 VLANs e suportar o protocolo IEEE 802.1Q.

2.24 Permitir a associação dinâmica de usuário a VLAN de acordo com parâmetros da etapa de autenticação.

2.25 Implementar Short Guard Interval.

2.26 Implementar Maximum Ratio Combining (MRC) ou MU-MIMO e para melhorar o desempenho de recepção.

2.27 Deve implementar mecanismo para detecção e prevenção ou minimização do impacto da interferência de sinais de radiofrequência não Wi-Fi na área de alcance do Ponto de Acesso.

2.28 Deve permitir a formação de conjuntos de Pontos de Acesso que se comuniquem e compartilhem as mesmas configurações mesmo sem a necessidade de uma controladora wireless (redes mesh).

2.29 Possuir capacidade de realizar análise de espectro de RF em 2.4 e 5 GHz para a detecção de outros pontos de acesso no perímetro de alcance, intrusos ou não autorizados (rogue), além de detectar interferências nos canais habilitados no

ponto de acesso.

2.30 Permitir a conexão de usuários utilizando os protocolos IPv4 e IPv6 simultaneamente no equipamento (dual-stack).

2.31 Deve suportar atribuição de endereço IP de forma estática e por meio de servidor DHCP.

2.32 Deve possibilitar a entrega automática de parâmetros de configuração a Pontos de Acesso que atendam critérios previamente definidos, de modo que toda configuração seja baixada do Controlador WLAN durante os processos de inicialização dos Pontos de Acesso.

2.33 Implementar os protocolos NTP ou SNTP em modo cliente, ou funcionalidade similar, para sincronização do relógio interno com fonte externa de tempo.

2.34 Permitir a configuração de VLans, criptografia e QoS independentes por SSID.

2.35 Implementar WIDS e WIPS, com recursos de assinaturas de ataques, detecção de dispositivos intrusos e aplicação de contramedidas de proteção.

2.36 Permitir autenticação pelo protocolo 802.1x com EAP-TLS.

2.37 Implementar solução de autenticação e gerenciamento de usuários da rede sem fios interna e independente da Controladora WLAN.

2.38 Possibilitar os métodos de autenticação de clientes: aberta (sem criptografia), através de MAC Address, WPA/WPA2/WPA3 em modos Personal e Entreprise com suporte a PSK e TKIP (para WPA e WPA2), AES (para WPA3), 802.1x por via de servidor Radius, 802.1x em base de dados local, 802.1x em base LDAP externa, Captive Portal.

2.39 Permitir a comutação de tráfego local (entre dispositivos da mesma sub-rede) sem necessidade de intervenção de Controladora WLAN, exceto para a fase de autenticação de usuários e estabelecimento da conexão inicial.

2.40 Ser gerenciável via protocolo SNMP v1/2c/3 e implementar MIB-II (RFC 1213).

2.41 Contar com garantia de 60 (sessenta) meses.

3. Ponto de Acesso (Access Point) Modelo 1

3.1 Suportar taxa de transmissão (PHY Rate) combinada entre 2.4Ghz e 5Ghz de, no mínimo, 1,45 Gbps.

3.2 Operar, pelo menos, em MIMO 2x2 com 2 fluxos espaciais SU-MIMO (2x2:2) em 2,4GHz e 5GHz.

3.3 Operar em canais de 20MHz para os padrões IEEE 802.11a/b/g, 20/40MHz para o padrão IEEE 802.11n e 20/40/80MHz para os padrões IEEE 802.11ac/ax.

4. Ponto de Acesso (Access Point) Modelo 2

4.1 Suportar taxa de transmissão (PHY Rate) combinada entre 2.4Ghz e 5Ghz de, no mínimo, 2,9 Gbps.

4.2 Operar, pelo menos, em MIMO 2x2 com 2 fluxos espaciais SU-MIMO (2x2:2) em 2,4GHz e MIMO 4x4 com 4 fluxos espaciais SU-MIMO e MU-MIMO (4x4:4) em 5GHz.

4.3 Operar em canais de 20MHz para os padrões IEEE 802.11a/b/g, 20/40MHz para o padrão IEEE 802.11n e 20/40/80/160MHz para os padrões IEEE 802.11ac/ax.

5. Injetor de energia PoE

5.1 Deve prover, por meio do cabo de rede UTP cat-5e ou cat-6, o fornecimento de energia capaz de alimentar os Access Points aqui descritos.

5.2 Deve possuir 2 portas RJ-45 fêmea, uma (entrada) para ser conectada à porta de dados do switch não PoE, outra (saída) para fornecer energia e dados para o Access Point. Ambas as portas devem operar sob o padrão Gigabit Ethernet.

5.3 Deve ser compatível com os padrões IEEE 802.3af e 802.3at e fornecer potência elétrica suficiente para que o dispositivo alimentado funcione com todas suas características ativas.

5.4 Deve acompanhar cabos e acessórios para o seu perfeito funcionamento.

5.5 Deve ser fornecido com fonte de alimentação com capacidade para operar em tensões de 110V ou 220V com comutação automática e frequência de 60Hz. Deve ser incluído cabo para conexão à rede elétrica no padrão brasileiro.

5.6 Garantia de 60 (sessenta) meses.

5.7 Este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos equipamentos dos itens 1.1 e 1.2 deste grupo (lote), ou ser homologado por este.

6. Controladora Wireless (*WLAN Controller*)

6.1 A Controladora Wireless (ou *WLAN Controller*) poderá ser ofertada em dispositivo físico (*hardware appliance*) ou virtualizado (*virtual appliance*), ou, ainda, em software aplicativo, deverá ser totalmente compatível com todas as funcionalidades e tecnologias e capaz de centralizar o controle, manutenção e distribuição das configurações dos Pontos de Acesso (Access Points) que compõem a solução.

6.2 Independentemente da arquitetura da Controladora Wireless (se dispositivo físico, virtualizado ou software aplicativo), esta deve poder ser instalada em Centros de Dados do Contratante juntamente com outra unidade idêntica, no mesmo local ou em local diverso, para compor um cluster e operar em modo de redundância e alta disponibilidade na forma ativo/ativo ou ativo/stand-by (Hot Stand-by) ou na proporção N+1 (onde sempre haja, além da quantidade mínima de nós necessária para suportar a demanda, mais uma unidade para prover redundância), possibilitando total redundância de configurações e replicação de sessões de usuários entre os equipamentos, de forma que se um dos nós sofra indisponibilidade, o outro assuma automática e integralmente a provisão de serviços, assegurando que não haja interrupção de funcionamento e da capacidade de gerenciamento dos dispositivos controlados.

6.3 Deve suportar e ser capaz de gerenciar todas as características e protocolos para os quais os Access Points adquiridos conjuntamente foram certificados, em especial:

6.3.1 Wi-Fi Certified a, b, g, n, ac, 6
6.3.2 WMM
6.3.3 WPA 3 Enterprise, Personal
6.3.4 WPA 2 Enterprise, Personal
6.3.5 Protected Management Frames

6.4 No caso da Controladora Wireless ser oferecida em dispositivo físico, o hardware deverá ser composto de pelo menos 2 interfaces de rede 10Gb Ethernet com porta SFP+ e respectivos transceivers 10GBASE-SR multimodo com conectores LC e 4 interfaces 10/100/1000 Mbps com conectores RJ-45 e oferecer throughput mínimo de tráfego de rede de 20Gbps.

6.5 A solução deverá poder controlar Pontos de Acesso que operem nos padrões IEEE 802.11a/b/g/n/ac/ax, com diferentes rádios, em quaisquer combinações desses padrões.

6.6 Cada Controladora Wireless deve ser capaz de gerenciar de forma nativa, simultaneamente, pelo menos 200 Pontos de Acesso, com centralização das funcionalidades de autenticação. Esta capacidade deve poder ser expandida por meio da adição de licenças de Pontos de Acesso e/ou por meio da adição de novas Controladoras Wireless a um cluster de controladoras conforme descrito no item 6.2, cujo gerenciamento deve ocorrer por meio de plataforma e interface de gerenciamento única.

6.7 A quantidade de Controladoras Wireless a ser fornecida deve ser

provisionada de acordo com o necessário e suficiente para gerenciar todos os Pontos de Acesso previstos em cada contratação.

6.8 Possuir capacidade de gerenciamento hierárquico, com possibilidade de definição de grupos de equipamentos e aplicação de alteração das características de configuração dos itens de todo o grupo sem a necessidade de configuração individual de cada equipamento.

6.9 Permitir operação dos Pontos de Acesso em modo de rede *wireless mesh*.

6.10 Permitir a configuração e o uso de múltiplos SSIDs simultaneamente em cada Ponto de Acesso, associando parâmetros de segurança distintos para cada SSID.

6.11 Ser capaz limitar o número de dispositivos conectados a cada Ponto de Acesso com base em parâmetro definido pelo administrador.

6.12 Permitir o envio ou a gravação em tempo real de registros de eventos e erros do sistema (logs) em servidor externo por meio do protocolo syslog ou equivalente.

6.13 Fornecer a visualização de alertas da rede em tempo real, com indicação do nível de severidade por cor.

6.14 Oferecer a capacidade de ser gerenciado através de navegador padrão (HTTP/HTTPS), SSH, e interface console (este último somente no caso da Controladora Wireless ser oferecida em dispositivo físico).

6.15 Suportar protocolos de transferência de arquivos como FTP (File Transfer Protocol) ou TFTP (Trivial File Transfer Protocol) ou SFTP (Secure File Transfer Protocol) ou SCP (Secure Copy Protocol).

6.16 Implementar protocolo de autenticação para controle do acesso administrativo à Controladora baseado em mecanismos de AAA (Authentication, Authorization and Accounting).

6.17 Permitir a criação de, pelo menos, dois grupos com níveis diferentes de permissão de acesso à Controladora Wireless, sendo um com capacidade de gerenciar todas as funções (administrativo) e outro apenas com permissão para visualização e/ou consulta de informações (somente leitura).

6.18 Ajustar dinamicamente canais e potência de radiofrequência dos Pontos de Acesso para otimizar a cobertura de rede e seu desempenho baseado na cobertura de APs vizinhos e interferências e implementar função de DFS e controle de TPC, conforme indicado no draft IEEE802.11h. Deve ser possível desabilitar o ajuste de potência e ajuste de canal automático.

6.19 Implementar, por meio dos Pontos de Acesso, varredura de RF periódica e automática, classificando fontes de interferência e APs não autorizados (rogues), evitando problemas de cobertura e controle da propagação indesejada de RF.

6.20 Deve permitir tráfego IPv4, IPv6 e Multicast através do controlador.

6.21 Suportar opções de comutação de tráfego central e comutação de tráfego local. Neste último modo não é necessário que todo o tráfego seja direcionado para a Controladora antes de ser encaminhado ao restante da rede, sendo possível a comunicação local, seja com recursos de rede (impressoras, servidores), seja com outros usuários WiFi sem o controle prévio da Controladora Wireless, otimizando a

conexão em caso de Pontos de Acesso gerenciados sobre um link remoto (internet, WAN, MPLS).

6.22 Deve controlar Pontos de Acesso em redes remotas, mesmo acessados por NAT ou através de túnel (VPN ou semelhante). Desta forma, deve ser possível definir o IP público da Controladora Wireless e fazer com que Pontos de Acesso remotos conectem-se automaticamente à Controladora Wireless através da Internet. Em caso de falha na comunicação entre Controladora Wireless e Ponto de Acesso, este deve continuar sua operação junto aos clientes já conectados.

6.23 Caso haja falha de comunicação entre os APs e a Controladora Wireless, os usuários associados devem continuar conectados à rede no mesmo SSID, ou seja, sem necessidade de reconexão em SSID diferente do que estava conectado. Também deve ser possível configurar a Controladora Wireless e os Pontos de Acesso para que novos usuários possam se conectar à rede utilizando autenticação 802.1x mesmo que os Pontos de Acesso estejam sem comunicação com a Controladora Wireless.

6.24 Deve permitir realizar o balanceamento automático da carga de usuários entre Pontos de Acesso adjacentes, fazendo a redistribuição de usuários entre os APs próximos sem intervenção humana e, no caso da inoperância de algum Ponto de Acesso, redistribuir automaticamente os usuários conectados a ele para os APs remanescentes dentro da área de alcance. Deve ser possível escolher em qual WLAN (SSID) será permitido executar tal ação.

6.25 Deve implementar funcionalidades de wIDS com intuito de controlar e identificar tentativas de ataques de tipos conhecidos ou identificáveis por regras heurísticas, e manter mecanismos que permitam atualizar a biblioteca de assinaturas de ataques.

6.26 Deve permitir implementar e gerenciar todos os recursos, assim como os mecanismos de segurança previstos no item Pontos de Acesso.

6.27 Deve implementar listas de controle de acesso (ACLs) para cada SSID dos Pontos de Acesso com restrições de endereço IP, tipos de protocolos, portas, QoS, VLAN e direção do fluxo de dados, com base nos parâmetros da etapa de autenticação. Deve ser possível a criação de ACLs para SSIDs de APs conectados local e remotamente.

6.28 Deve ser possível determinar, por SSID, se os usuários conectados a determinado SSID poderão ou não trocar pacotes entre si.

6.29 Implementar segurança baseada nos padrões WPA/WPA2/WPA3 e 802.11i.

6.30 Possuir suporte a autenticação IEEE 802.1x, com pelo menos três dos seguintes métodos EAP: EAP-MD5, PEAP/EAP-GTC, EAP-PEAP, PEAP/EAP-MSCHAPv2, EAP-TLS com utilização de base de usuários interna ou servidor RADIUS externo.

6.31 Deve possuir funcionalidade de portal de autenticação web (Captive Portal), sendo possível indicar um Captive Portal externo e, também, implementar um Captive Portal interno, caso em que todo o mecanismo de autenticação deve ser interno à Controladora Wireless (website, lista de usuários, políticas). Além disso, deve ser possível a criação de páginas personalizadas com imagem e texto, e

especificar o tempo que um determinado usuário (login) ficará válido para ter acesso a rede através da autenticação web.

6.32 Deve permitir o cadastramento de usuários visitantes na base interna da Controladora Wireless.

6.33 Deve permitir a criação, pelos administradores, de perfis de tráfego para aplicações de voz e vídeo e permitir a priorização deste tráfego com atribuição de QoS.

6.34 A solução deve ainda permitir a criação de regras para bloqueio e limite de banda de aplicações comuns de mercado e que estas regras possam ser aplicadas por SSID ou grupos de usuários.

6.35 Deve implementar recurso que evite automaticamente a conexão de usuários wireless em Pontos de Acesso classificados como maliciosos ou não autorizados.

6.36 A solução deve permitir detectar e/ou mitigar interferências que impactem diretamente no funcionamento da rede.

6.37 Deve permitir implementar configurações distintas por SSID nos Pontos de Acesso, locais ou remotos, tais como regras de autenticação, QoS, criptografia, SSID e VLAN. Deve ser possível especificar em quais APs/Grupos de APs cada SSID será aplicado.

6.38 Para fins de controle, deve permitir a restrição da quantidade de usuários conectados em um determinado SSID.

6.39 Deve permitir o gerenciamento da disponibilidade de SSIDs por data/hora e dias da semana e horários previamente determinados.

6.40 Possibilitar fast roaming, melhorando a performance de aplicações em tempo real (802.11r).

6.41 Implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente Pontos de Acesso próximos disponíveis para roaming.

6.42 Deve implementar SNTP ou NTP para sincronização de tempo com outros dispositivos de rede.

6.43 Deve permitir a atualização do software (firmware) da Controladora Wireless e do software (firmware) dos Pontos de Acesso (APs), mesmo quando conectado remotamente.

6.44 Implementar SNMP v2c e v3 incluindo a geração de traps, a criptografia do tráfego de dados de gerência e suportar MIB vII (conforme RFC 1213), que permitam coletar dados de uso pelo menos dos seguintes componentes da Controladora e dos Pontos de Acesso: interfaces de rede, CPU e memória.

6.45 Deve implementar os protocolos IPv4 e IPv6 (dual stack).

6.46 Deve suportar Wireless Multimedia Extensions (WMM).

6.47 Oferecer detecção e proteção integrada de ataques de negação de serviços.

6.48 Implementar Qualidade de Serviço com a marcação de pacotes utilizando Diffserv e suporte a 802.1p para QoS de rede.

6.49 Deve reconhecer e ser capaz de aplicar políticas de QoS para otimização de tráfego de aplicações.

6.50 Permitir o controle de banda disponível (bandwidth contracts) por usuário ou através de perfis de usuários.

6.51 Possuir capacidade de gerar alarmes e executar contramedidas no caso de detecção de um ataque.

6.52 Implementar o protocolo 802.1w (Rapid Spanning Tree) no caso da Controladora Wireless ser oferecida em dispositivo físico.

6.53 Poder atuar como Proxy Arp

6.54 Oferecer os recursos de roaming de camada L2.

6.55 Implementar tagging de VLANs através do protocolo 802.1Q.

6.56 Ser capaz de realizar a descoberta automática dos APs na infraestrutura wireless.

6.57 Ser capaz de estabelecer conexão tunelada entre Pontos de Acesso e Controladora Wireless de maneira segura.

6.58 Possuir capacidade de consulta em tela ou geração de relatórios dos seguintes tipos de informação: Listagem de Pontos de Acesso ativos, listagem de clientes wireless ativos por Ponto de Acesso, por grupos de Pontos de Acesso e por SSID, taxa de utilização de rede por Ponto de Acesso.

6.59 Qualquer das funcionalidades acima pode ser considerada suprida caso esteja disponível na Solução de Controle de Acesso à Rede (NAC).

7. Solução de Controle de Acesso à Rede (NAC)

7.1 A Solução de Controle de Acesso à Rede (NAC), doravante chamada de NAC, deverá ser totalmente compatível e ter capacidade de gerenciar, de maneira integrada, todas as funcionalidades e tecnologias da Controladora Wireless e dos Pontos de Acesso que compõem a Solução de Rede Wi-Fi, podendo ser utilizada como única interface gráfica de administração de toda solução descrita neste documento ou ser composta de um ou mais softwares do mesmo fabricante.

7.2 Será aceito que a Solução de Controle de Acesso à Rede (NAC) seja física (*hardware appliance*) ou virtualizada (*virtual appliance*) ou, ainda, software aplicativo instalável em servidor Microsoft Windows Server 2019 ou superior ou GNU Linux, ou, ainda, conjunto de funcionalidades de gerenciamento existentes na Controladora Wireless, ativas e disponíveis por padrão ou ativáveis por licenciamento.

7.3 **Caso a Controladora Wireless a ser ofertada ofereça todas as funcionalidades de gerenciamento exigidas neste item, sem custo ou necessidade de licenciamento adicional, o proponente deve mencionar explicitamente isso em sua proposta e cotar este item com o custo simbólico R$ 1,00.**

7.4 Deve suportar e ser capaz de gerenciar todas as características e protocolos para os quais a Controladora Wireless os Access Points adquiridos conjuntamente foram certificados, em especial:

7.4.1 Wi-Fi Certified a, b, g, n, ac, 6
7.4.2 WMM
7.4.3 WPA 3 Enterprise, Personal
7.4.4 WPA 2 Enterprise, Personal
7.4.5 Protected Management Frames

7.5 O software deve contar com um mínimo de 1.000 licenças de uso e autenticação para usuários/dispositivos internos à rede corporativa e mais 500 licenças de uso e autenticação para usuários/dispositivos visitantes e deve, ainda, poder ter a quantidade de usuários/dispositivos licenciados acrescida pela mera aquisição e registro de novas licenças, sem a necessidade de qualquer reinstalação ou alteração nos softwares instalados.

7.6 No caso da Solução de Controle de Acesso à Rede (NAC) ser oferecida em dispositivo físico, o hardware deverá ser composto de pelo menos 1 interface de rede Multigigabit Ethernet 2.5Gb e 2 interfaces 10/100/1000 Mbps com conectores RJ-45 e oferecer throughput mínimo de tráfego de rede de 2Gbps.

7.7 Deve permitir que todos os eventos da Controladora Wireless e dos Access Points sejam redirecionados para uma console de gerência central.

7.8 Toda a interface de gerenciamento deverá ser gráfica e o acesso ao sistema deverá ser por meio de cliente com browser padrão, compatível com Microsoft Edge, Google Chrome e Mozilla Firefox em suas versões mais recentes, utilizando o protocolo HTTPS.

7.9 . Implementar protocolo de autenticação para controle do acesso administrativo à solução utilizando servidor Radius e auditoria de comandos com

mecanismos de AAA.

7.10 Possuir visualização dos mapas de calor (heatmaps) dos andares de cada prédio, apresentando, em tempo real, posição dos pontos de acesso, dos clientes conectados, dos rogue APs e a cobertura do sinal de radiofrequência tanto em 2,4 GHz como em 5 GHz.

7.11 Permitir a visualização de eventuais áreas sem cobertura de radiofrequência (áreas de sombra).

7.12 Permitir a monitoração do desempenho, em tempo real, das redes WLAN, reportando os seguintes parâmetros: falhas de autenticação, relação sinal-ruído, interferência, potência de sinal, utilização da rede por cliente dos e APs e consumo de CPU e memória nas Controladoras Wireless.

7.13 Deve implementar a listagem em tempo real das informações dos usuários conectados nas redes WLAN contendo os seguintes parâmetros: endereço IP, endereço MAC, banda utilizada pelo cliente, nível de potência de recepção, relação sinal-ruído, parâmetros de associação, autenticação e nome do usuário.

7.14 Possuir capacidade de identificação e listagem dos rádios vizinhos e respectivos SSID/BSSID que causam interferência na rede sem fio.

7.15 Possuir capacidade de gerenciamento hierárquico com possibilidade de definição de grupos de equipamentos e alteração das características de configuração do grupo sem a necessidade de configuração individual de cada equipamento.

7.16 Implementar modelos de configuração (templates) de forma a possibilitar a replicação de configuração aos equipamentos selecionados.

7.17 Realizar a descoberta automática dos dispositivos individuais da infraestrutura wireless.

7.18 Fornecer a visualização de alertas da rede em tempo real, com indicação do nível de severidade por cor.

7.19 Ser capaz de detectar, em conjunto com a Controladora Wireless e os Pontos de Acesso, pelo menos, os seguintes ataques: flood de frames de gerenciamento dos clientes wireless, respostas de null probe, flood de autenticação, ataque de deauthentication, flood de EAP handshake.

7.20 Implementar mecanismos para detecção, localização e bloqueio de pontos de acesso não autorizados (rogue) e redes ad-hoc.

7.21 Deve possuir ferramenta para de ajuste automático de configurações de espectro, onde configure, no mínimo, os seguintes parâmetros, baseados em dados colhidos dos próprios Pontos de Acesso:

7.21.1 Potência do rádio

7.21.2 Canal de difusão

7.22 Possuir capacidade de consulta em tela ou geração de relatórios dos seguintes tipos de informação: Listagem de clientes wireless por período informado, informações de configuração das Controladoras Wi-Fi, utilização da rede, detalhes dos pontos de acesso não autorizados (rogues) detectados.

7.23 Deve possuir consulta em tela ou relatório que permita identificar a versão

de software instalada e o número serial de todos os equipamentos monitorados na plataforma.

7.24 A plataforma deve ser capaz de analisar, a nível de protocolo, falhas no momento de autenticação, ajudando a identificar a etapa da autenticação em que houve a falha

7.25 A plataforma deve ser capaz apresentar em tempo real a quantidade de usuários conectados a um agrupamento lógico de Pontos de Acesso, que possam representar uma determinada sala, andar ou localidade de interesse.

7.26 A plataforma deve ser capaz de identificar e apresentar dados de usuários que estão com baixa qualidade de serviços na rede.

7.27 Deve ser capaz de apresentar painel com as aplicações (em camada 7 do modelo OSI) que estão sendo executadas na rede e mostrar o consumo de banda por aplicação.

7.28 A plataforma deve ser capaz de detectar interferências, aplicar contramedidas, e identificar o Ponto de Acesso no qual a interferência foi detectada.

7.29 Deve ser possível, através da plataforma de gerência, acessar o terminal de comando ou determinar a execução de scripts CLI nos Pontos de Acesso gerenciados.

7.30 Deve permitir a criação de perfis de administradores, criando visões administrativas independentes como, por exemplo, administradores (acesso completo à plataforma), operadores (acesso a configurações de usuários e Pontos de Acesso) e monitores (acesso apenas de leitura a consultas, painéis e relatórios).

7.31 Deve permitir a atualização remota do sistema operacional e dos arquivos de configuração utilizados nos Pontos de Acesso, Controladoras Wireless a partir da Solução de Gerência

7.32 Deve realizar a atualização de software do conjunto de Controladoras Wireless e Pontos de Acesso de forma gradual (em grupos), sem causar indisponibilidade do respectivo serviço.

7.33 Deve permitir implementar autenticação 802.1x para os usuários da rede sem fios utilizando, pelo menos, o método EAP-TLS.

7.34 Deve permitir a integração com RADIUS Server com suporte ao método EAP citado no item anterior.

7.35 Deve implementar autenticação RADIUS baseada em endereço MAC (Radius-based MAC authentication) dos dispositivos clientes.

7.36 Deve implementar autenticação via portal web (captive portal) para os usuários da rede que não puderem se autenticar via 802.1x. O serviço web de autenticação (captive portal) deve ser fornecido e hospedado dentro da solução ofertada, além de permitir que as requisições possam ser redirecionadas para um serviço externo.

7.37 Permitir processo de conexão segura à rede sem fio através da instalação de certificado digital e configuração de perfil de rede sem fio em dispositivos móveis. A solução deve identificar o tipo de dispositivo cadastrado e conectado à rede para que seja possível provisionar o certificado digital e configurar o perfil da rede sem fio conforme o sistema operacional utilizado, no mínimo os seguintes sistemas

operacionais: Android , Apple iOS, Mac OS X e Windows, para que o usuário utilize autenticação segura via 802.1X na rede corporativa.

7.38 Para redes abertas (guest VLAN) utilizadas em eventos e para visitantes, o cliente deverá poder se conectar sem senha à infraestrutura de rede e ter seu acesso redirecionado para o portal de autenticação.

7.39 O Captive Portal deve permitir a customização das páginas web do portal, com a inclusão de imagens, instruções em texto e campos de texto que devem ser preenchidos pelos clientes.

7.40 O Captive Portal deve possuir suporte aos idiomas Português do Brasil ou Inglês, quando não houver em idioma Português, a plataforma deve permitir que seja realizado a tradução.

7.41 Deve suportar diferentes tipos de servidores de AAA (Authentication, Authorization and Accounting) de retaguarda (“Backend Authentication Servers”), como RADIUS, LDAP e Microsoft Active Directory (sem alteração no Schema do AD).

7.42 Deve implementar funcionalidades de Classificação Automática de Dispositivos (“Device profiling”), de forma a descobrir, classificar e agrupar os dispositivos conectados na rede, permitindo extrair informações de contexto que devem ser usadas na aplicação de políticas de acesso.

7.43 Deve implementar gerenciamento e aplicação de políticas de autorização de acesso de usuários com base em:

7.43.1 Grupo do usuário no Active Directory

7.43.2 Protocolo de autenticação utilizado

7.43.3 Tipo de dispositivo utilizado

7.43.4 Localização ou região do AP em que se conectou

7.44 Deve implementar os serviços de autenticação, profiling, provisionamento e autorização para, pelo menos, 1.500 mil usuários/dispositivos simultâneos.

7.45 Possuir plataforma unificada que combina AAA, NAC, BYOD e acesso de convidado incorporando identidade, integridade, informações físicas / de dispositivo e elementos condicionais em um conjunto de políticas.

7.46 Suporte a seguintes fontes para autenticação:

7.46.1 Microsoft Active Directory

7.46.2 Kerberos

7.46.3 LDAP-compliant directory

7.46.4 Radius

7.46.5 Microsoft Azure Active Directory

7.46.6 Google G Suite

7.46.7 Lista estática de endereços MAC

7.47 Deve suportar "Single Sign-on" (SSO) através de SAML v2.0 ou NPS

(Network Policy Server).

7.48 Deve implementar gerenciamento e aplicação de políticas de autorização de acesso de usuários com base em:

7.48.1 Atributos do usuário autenticado,

7.48.2 Hora do dia, dia da semana,

7.48.3 Tipo de dispositivo utilizado,

7.48.4 Localização do usuário;

7.48.5 Tipo de autenticação utilizado

7.49 Permitir a visualização de todas informações relativas a cada usuário conectado, como data e hora de autenticação, MAC Address do dispositivo, classificação do dispositivo, usuário, equipamento que requisitou a autenticação (origem), método de autenticação utilizado, fonte de autenticação utilizada para validação, status da autenticação e alertas em caso de falha.

7.50 Deve implementar funcionalidade de classificação automática de dispositivos (“Device profiling”), de forma a descobrir, classificar e agrupar os dispositivos conectados na rede;

7.51 Deve categorizar os dispositivos em pelo menos 3 níveis, por tipo de dispositivo (ex. Computador, Smartphone, impressora, etc), por sistema operacional (ex. Windows, Linux, MacOS, etc.) e versão do sistema (ex. Windows 7, Windows 2008 Server, etc);

7.52 Deve suportar a coleta de informações, para classificação, usando no mínimo 2 dos métodos a seguir: DHCP, HTTP User-Agent, MAC OUI, ActiveSync plugin, SNMP, Subnet Scanner, IF-MAP, Cisco Device Sensor, MDM e TCP Fingerprinting;

7.53 Deve possuir base de categorias de dispositivos pré-configuradas e suportar a criação de regras para os dispositivos de acordo com sua categoria;

7.54 Deve implementar os serviços de autenticação, profiling e autorização para 1.500 usuários/dispositivos;

7.55 Deve permitir que cada dispositivo receba uma chave pré-compartilhada exclusiva durante o registro do dispositivo.

7.56 Suporte a RADIUS CoA, Web authentication e SAML v2.0 ou NPS (Network Policy Server).

7.57 Suporte a aplicação de políticas em ambiente multivendor de Wireless, cabeado e VPN.

7.58 Deve permitir configurar um meio para proteger a comunicação entre clientes RADIUS / TCP na camada de transporte, utilizando TLS para encriptação da comunicação.

7.59 Deve suportar EDUROAM

7.60 Suporte a integração com plataforma de terceiros usando HTTP/RESTFUL API.

7.61 Permitir que a solução faça consultas em bases internas de usuários, com o objetivo de buscar informações a serem utilizadas durante o processo de

autenticação dos usuários.

7.62 A solução deve permitir configuração em alta disponibilidade com no mínimo dois elementos, seja em modo ativo/ativo ou ativo/stand-by.

7.63 A solução deve permitir a configuração centralizada de políticas em ambientes distribuídos, na qual as políticas serão configuradas em um único elemento para serem distribuídas aos demais que pertençam à mesma "zona".

7.64 Gerenciamento de Usuários Visitantes (Convidados):

7.64.1 Deve possuir ferramenta para gerenciar os processos de credenciamento, autenticação, autorização e contabilidade de usuários visitantes através de um portal web seguro;

7.64.2 Deve implementar a criação de grupos de autorizadores com privilégios distintos de criação de credenciais temporárias e atribuição de permissões de acesso aos clientes;

7.64.3 Deve realizar a autenticação dos autorizadores em base externa do tipo Microsoft Active Directory ou LDAP e atribuir o privilégio ao autorizador de acordo com o seu perfil;

7.64.4 Deve implementar as funcionalidades de geração aleatória de lotes de credenciais temporárias pré-autorizadas;

7.64.5 Deve implementar a importação e exportação da relação de credenciais temporárias através de arquivos txt, csv, xls ou xlsx;

7.64.6 Deve permitir a criação de validade das credenciais, baseando o início da validade na criação da conta ou no primeiro login da conta;

7.64.7 Deve permitir que o visitante crie sua própria credencial temporária (“self-service”) através do portal web, sem a necessidade de um autorizador;

7.64.8 Deve permitir a customização do formulário de criação de credenciais, a ser preenchido pelo autorizador ou pelo visitante, em caso de autosserviço, especificando quais informações cadastrais dos visitantes são obrigatórias ou opcionais;

7.64.9 Deve implementar algum nível de segurança da senha temporária que será gerada ao visitante, como a exigência de uma quantidade mínima de caracteres ou o uso da combinação de caracteres especiais e números para compor a senha;

7.64.10 Deve exigir que o usuário visitante aceite o “Termo de uso da rede” a cada login ou apenas no primeiro login;

7.64.11 Deve permitir o envio das credenciais aos usuários registrados através de mensagens SMS (Short Message Service), email e impressão local

7.64.12 Deve permitir que a customização da página de registro de

visitantes para campos relacionados a confirmação de sponsorship;

7.64.13 Deve permitir o gerenciamento das credenciais de visitantes;

7.64.14 Deve permitir a configuração de contas de usuários visitantes com as seguintes características: Prazo de validade, largura de banda;

7.64.15 Deve realizar o caching de endereço MAC dos usuários visitantes;

7.64.16 Deve permitir o login automático de usuários que realizem o auto-registro;

7.64.17 Deve permitir a autenticação de usuário anônimo sem necessidade de prover usuário e senha;

7.64.18 Deve permitir a criação de token ou QR Code de acesso;

7.64.19 Deve permitir a criação e gerenciamento de múltiplas contas de usuários visitantes;

7.64.20 Deve permitir a desconexão de múltiplas sessões ativas;

7.64.21 Deve permitir autenticação através de social login nativa na solução;

7.65 Deve ser capaz de modificar ou desconectar uma sessão ativa de visitante através de RADIUS Dynamic Authorization.

7.66 Qualquer das funcionalidades acima pode ser considerada suprida caso esteja disponível na Controladora Wireless.

8. Pacote de licenças adicionais de usuários corporativos

8.1 Conjunto de autorizações de uso, autenticação e/ou acesso (licenças) que, quando agregadas à Solução de Controle de Acesso à Rede (NAC), expandem quantitativamente sua capacidade de suportar, autenticar, controlar e gerenciar um maior número de usuários/dispositivos na rede sem fios com acesso aos recursos ou perfis de segurança internos daquela rede;

8.2 Deve ser constituída por elemento de autorização ou chave de acesso agregável ao software descrito no item Solução de Controle de Acesso à Rede ou, ainda, Controladora Wireless, a depender da configuração da plataforma do fabricante sem, todavia, requerer a adição de novos componentes de hardware ou software e nem tampouco afetar o funcionamento de qualquer elemento previamente existente a não ser pela própria expansão da capacidade de atendimento a novos usuários/dispositivos.

8.3 Deverá ser comercializada e precificada em pacotes de autorização/licenciamento para 500 usuários/dispositivos adicionais em cada unidade ofertada. **Caso a Solução de Controle de Acesso a Rede (NAC) a ser ofertada ofereça acesso irrestrito/ilimitado a qualquer quantidade de usuários sem custo ou necessidade de licenciamento adicional, o proponente deve mencionar explicitamente isso em sua proposta e cotar este item com o custo simbólico R$ 1,00.**

9. Pacote de licenças adicionais de usuários visitantes

9.1 Conjunto de autorizações de uso, autenticação e/ou acesso (licenças) que, quando agregadas à Solução de Controle de Acesso à Rede (NAC), expandem quantitativamente sua capacidade de suportar, autenticar, controlar e gerenciar um maior número de usuários/dispositivos na rede sem fios sem acesso aos recursos ou perfis de segurança internos daquela rede, caracterizados como aqueles que são submetidos aos processos de autenticação e gerenciamento de acesso descritos no item 7.64;

9.2 Deve ser constituída por elemento de autorização ou chave de acesso agregável ao software descrito no item Solução de Controle de Acesso à Rede ou, ainda, Controladora Wireless, a depender da configuração da plataforma do fabricante sem, todavia, requerer a adição de novos componentes de hardware ou software e nem tampouco afetar o funcionamento de qualquer elemento previamente existente a não ser pela própria expansão da capacidade de atendimento a novos usuários/dispositivos.

9.3 Deverá ser comercializada e precificada em pacotes de autorização/licenciamento para 500 usuários/dispositivos adicionais em cada unidade ofertada. **Caso a Solução de Controle de Acesso a Rede (NAC) a ser ofertada ofereça acesso irrestrito/ilimitado a qualquer quantidade de usuários sem custo ou necessidade de licenciamento adicional, o proponente deve mencionar explicitamente isso em sua proposta e cotar este item com o custo simbólico R$ 1,00.**

10. Entrega e instalação

10.1 Todos os equipamentos e softwares descritos nos itens 3, 4, 5, 6, 7, 8 e 9 acima deverão ser entregues no Complexo Sede do Tribunal Regional do Trabalho da 23ª Região.

10.2 O prazo de entrega para os bens referidos no item 10.1 é de 90 dias após Ordem de Serviço.

10.3 Imediatamente após a Ordem de Serviço, a Contratada terá 20 dias para elaboração do projeto executivo de instalação da Rede Sem Fios, que contemplará todas as etapas do processo, desde o cronograma da instalação e as datas previstas para a realização de cada etapa, contendo pelo menos os seguintes eventos:

10.3.1 Site Survey presencial **prévio** no Site Piloto;

10.3.2 Apontamento dos locais de instalação dos Pontos de Acesso do Grupo Piloto

10.3.3 Instalação e ativação da controladora e Solução de Controle de Acesso à Rede (NAC);

10.3.4 Instalação e ativação dos Pontos de Acesso do Grupo Piloto;

10.3.5 Validação das configurações e parâmetros de operação do Site Piloto;

10.3.6 Site Survey presencial **pós** instalação no Site Piloto;

10.3.7 Realização da capacitação “Hands-on”;

10.3.8 Site Survey virtual nos demais ambientes da contratante;

10.3.9 Apontamento dos locais de instalação dos demais Pontos de Acesso;

10.3.10 Ativação remota dos demais pontos de acesso;

10.3.11 Validação da instalação e funcionamento de toda a rede.

10.4 O projeto executivo de instalação da Rede Sem Fios deverá ser entregue ao Gestor do Contrato, que o submeterá à análise do Fiscal Técnico para aprovação em até **5 dias úteis**. Em caso de reprovação do projeto ou apontamento da necessidade de alterações, a contratada terá **5 dias úteis** após a notificação para promover as alterações demandadas e entregar a versão definitiva do projeto.

10.5 Para fins de planejamento, provisionamento de recursos e estimativa de custos, fica determinado que os serviços de instalação consistirão em:

10.5.1 Instalação das Controladoras Wireless (item 6);

10.5.2 Instalação da Solução de Controle de Acesso de Rede (item 7);

10.5.3 Realização de Site Survey presencial prévio no Site Piloto;

10.5.4 Instalação e/ou ativação lógica e configuração dos primeiros 50 Pontos de Acesso (itens 3 e/ou 4) instalados fisicamente no(s) prédio(s) da Sede do Tribunal contratante (ou até este limite) e da ativação lógica e configuração dos demais Pontos de Acesso

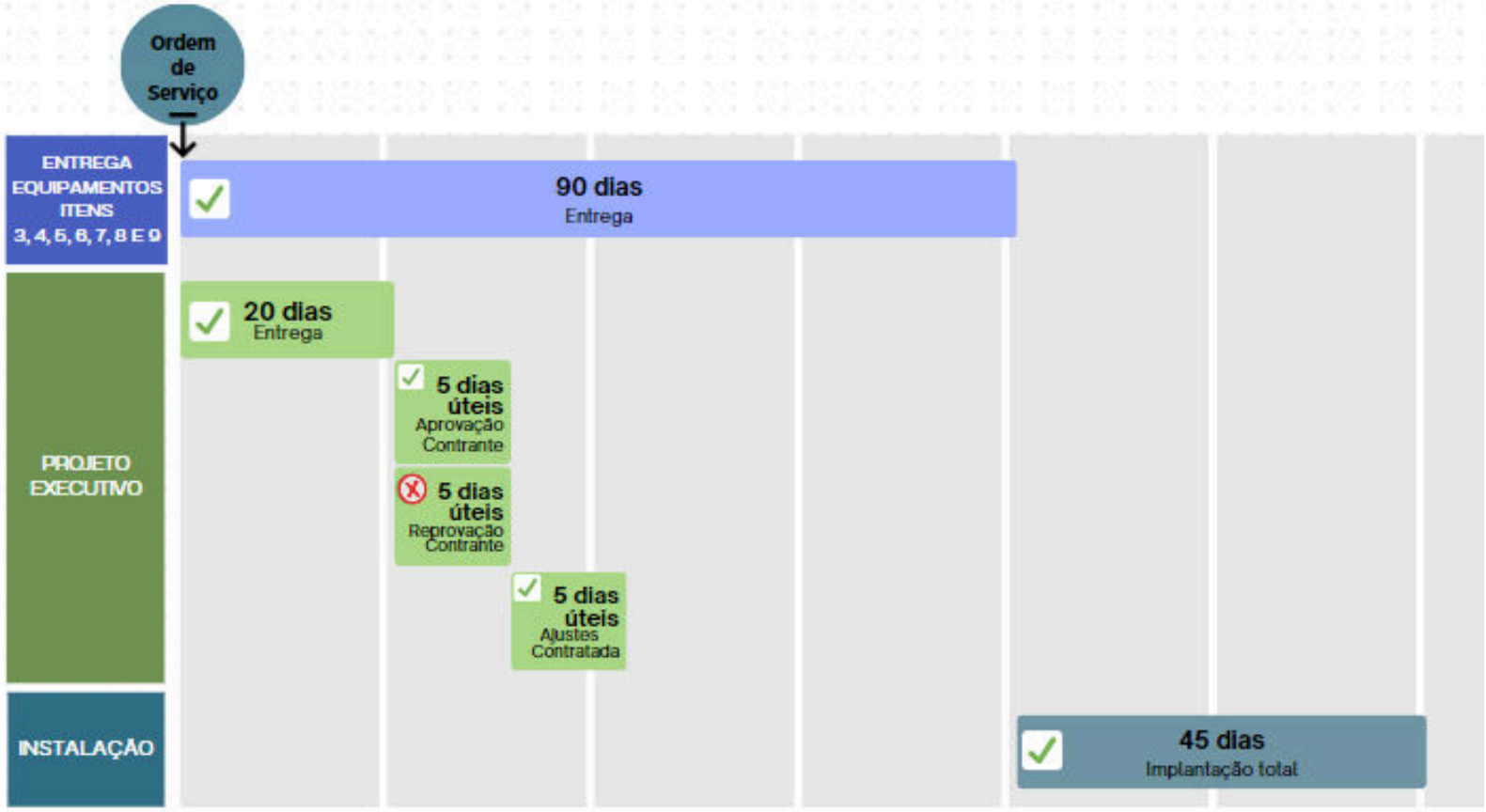
10.5.5 Realização de Site Survey presencial pós instalação no Site piloto;

10.6 Fica esclarecido que o Site Piloto será definido pela equipe de Gestão do Contrato e abrangerá apenas os ambientes da sede da contratante que sejam suficientes e necessários para a instalação da Controladora Wireless, da Solução de Controle de Acesso de Rede e de um conjunto de até 50 Pontos de Acesso que comporão o assim chamado Grupo Piloto de ativação.

10.7 Fica esclarecido, ainda, que a instalação física, provimento de cabeamento de rede e eventual alimentação elétrica de todos os Pontos de Acesso serão de inteira responsabilidade do contratante e deverá ser realizada até a data prevista no projeto executivo para a ativação lógica desses mesmos Pontos de Acesso.

10.8 O prazo final da implantação é de até 45 dias após a entrega dos bens referidos no item 10.1.

10.9 Em virtude da necessidade de provimento, pela contratante, da infraestrutura para a instalação física dos Pontos de Acesso, serão aceitos como implantados os demais APs, aqueles que não foram instalados no Site Piloto, desde que plenamente configurados e testados em bancada para posterior distribuição pela contratante.


Ordem de Serviço
ENTREGA EQUIPAMENTOS ITENS 3, 4, 5, 6, 7, 8 E 9
90 dias
Entrega
PROJETO EXECUTIVO
20 dias
Entrega
5 dias úteis
Aprovação Contrante
5 dias úteis
Reprovação Contrante
5 dias úteis
Ajustes Contratada
INSTALAÇÃO
45 dias
Implantação total

11. Transferência de conhecimento "*hands on*"

11.1 A transferência de conhecimento na modalidade "*hands on*" deverá ocorrer de maneira presencial, imediatamente após a instalação dos componentes de hardware e software da Controladora Wireless e Solução de Controle de Acesso à Rede (NAC), juntamente com a instalação do Grupo Piloto de Pontos de Acesso no ambiente.

11.2 A capacitação aqui descrita deverá contar com uma carga-horária mínima de 24h, dentre as quais, pelo menos 50% sejam compostas por atividades práticas.

11.3 A capacitação deverá ser conduzida por profissional certificado (com certificação de proficiência) oficialmente pelo fabricante da Solução, para todos os itens que a compõem (Pontos de Acesso, Controladora Wireless e Solução de Controle de Acesso). Caso um único profissional não possua certificação oficial de todos os componentes, será aceita a condução por uma equipe de profissionais com certificação em partes complementares da solução.

11.4 A capacitação deverá contar com material de apoio orientativo contendo a relação das atividades, seus objetivos e descrição, e ser elaborado pelo instrutor ou organização promovente, e ser entregue aos alunos em formato eletrônico ou impresso.

11.5 O conteúdo da capacitação deverá no mínimo abranger, mas não se restringir a, todos os aspectos fundamentais de instalação, configuração, ativação, operação, diagnóstico e resolução de problemas (troubleshooting) dos componentes adquiridos e que constituirão a Rede Sem Fios, em um nível de profundidade de conhecimento equiparável ao que a Biblioteca ITIL considera as habilidades de uma equipe de suporte de Nível 1.

11.6 Após a conclusão da capacitação, deverá ser realizada uma pesquisa de satisfação onde os participantes possam avaliar com notas objetivas e comentários discursivos a qualidade do conteúdo, dos materiais de apoio e do(s) instrutor(es). Caso o resultado geral apurado por média aritmética seja inferior a 75% de aprovação, a capacitação deverá ser reformulada considerando os pontos de menor nota na avaliação e realizada novamente em um prazo inferior a 30 dias.

11.7 A capacitação poderá ser realizada de forma presencial na sede da contratante, em ambiente fornecido por ela, ou em ambiente fornecido pela contratada na mesma cidade da sede da contratante. A capacitação também poderá ser realizada de forma telepresencial síncrona em ambiente virtual de aprendizagem com a participação simultânea do instrutor e dos treinandos.

11.8 A capacitação poderá ser realizada por profissionais diretamente vinculados à contratada ou por meio do fornecimento de vouchers de treinamentos oficiais do fabricante.