

## **Anexo II - Especificações Técnicas - Projeto Técnico**

### **Objeto**

Contratação de empresa para aquisição, instalação, configuração, manutenção e garantia de ponto de acesso WiFi com solução de controladora wireless em nuvem para a Rede Pública de Educação do Estado de São Paulo.

## Índice

1	OBJETIVO .....	4
2	OBJETIVOS ESPECÍFICOS .....	4
3	JUSTIFICATIVA .....	4
4	ESPECIFICAÇÃO TÉCNICA DOS EQUIPAMENTOS E SERVIÇOS .....	5
4.1	PONTO DE ACESSO WIFI A/B/G/N/AC WAVE 2 INDOOR .....	5
5	ESPECIFICAÇÃO TÉCNICA DOS SERVIÇOS DE INSTALAÇÃO .....	12
5.1	INSTALAÇÃO E CONFIGURAÇÃO DO PONTO DE ACESSO WIFI NA ESCOLA .....	12
6	GARANTIA .....	13
6.1	CARACTERÍSTICAS GERAIS .....	14
7	CAPACITAÇÃO.....	15
7.1	CARACTERÍSTICAS GERAIS .....	15
7.2	CAPACITAÇÃO TÉCNICA .....	16
8	HOMOLOGAÇÃO.....	17

## 1 Objetivo

Atualmente a Secretaria da Educação do Estado de São Paulo disponibiliza vários sistemas web para os professores e alunos da rede pública de ensino, como por exemplo, o secretaria escolar digital (<https://sed.educacao.sp.gov.br/>), CurrículoMais (<http://curriculomais.educacao.sp.gov.br/>), portal da educação ([www.educacao.sp.gov.br/](http://www.educacao.sp.gov.br/)), capacitação de professores (<http://www.escoladeformacao.sp.gov.br/>), entre outros.

Como estes sistemas estão disponíveis na internet, é preciso facilitar o meio de acesso a estas plataformas nas escolas. Tendo isto em pauta, este projeto tem como objetivo, disponibilizar uma rede Wireless autenticada para que alunos, professores e servidores possam acessar a internet de forma segura e controlada. Esta iniciativa, por meio da incorporação de novas tecnologias a serviço da aprendizagem, visa alavancar o desempenho escolar dos alunos e prepará-los para os novos desafios da era digital e do conhecimento.

## 2 Objetivos Específicos

A seguir estão descritos os objetivos específicos deste projeto:

- Preparar os alunos para a era digital e do conhecimento por intermédio da tecnologia.
- Disponibilizar acesso sem fio e controlado à Internet para os professores e alunos das unidades escolares públicas do Estado de São Paulo;
- Implantar uma rede WiFi com autenticação baseada em usuário;
- Implantar uma infraestrutura de rede WiFi escalável e adaptável a mudanças para a Rede Pública de Educação do Estado de São Paulo.

## 3 Justificativa

A Secretaria da Educação com apoio da FDE vem trabalhando para manter e melhorar a rede de dados das escolas. No intuito de disponibilizar um acesso mais flexível e com controle, a fim de atender aos objetivos dos Programas de Tecnologias da Secretaria de Estado da Educação de São Paulo, surgiu a necessidade de criar uma rede WiFi, onde cada aluno e professor acessará a internet através da rede sem fio por meio de usuário e senha particular.

## **4 Especificação Técnica dos Equipamentos e Serviços**

Serão aceitos produtos que atendam exatamente ou que excedam este conjunto mínimo de exigências.

Para todos os itens que representem bens materiais a contratada deverá fornecer produtos novos, sem uso anterior. Além disso, devem estar em linha de produção e sem previsão de encerramento de fabricação na data de entrega da proposta.

Todos os softwares e equipamentos ofertados devem ser do mesmo fabricante, afim de garantir uma perfeita interoperabilidade.

O prazo para entrega, instalação e configuração dos equipamentos será de até 30 dias a contar da data de assinatura da Ordem de Fornecimento/Serviço.

### **4.1 Ponto de Acesso WiFi A/B/G/N/AC WAVE 2 Indoor**

#### **4.1.1 Condição de Fornecimento**

- 4.1.1.1 Deverão ser fornecidos pontos de acesso WiFi idênticos, novos e sem uso anterior. O modelo ofertado deverá estar em linha de produção, sem previsão de encerramento, na data de entrega da proposta. Não serão aceitos modelos de ponto de acesso destinados a implementação em ambientes de baixa densidade de clientes WiFi.
- 4.1.1.2 A configuração dos seus parâmetros operacionais, o gerenciamento das políticas de segurança e de radiofrequência devem ser gerenciadas por uma solução de Controladora Wireless em nuvem. Esta solução de controladora wireless em nuvem deverá ser do mesmo fabricante do ponto de acesso afim de garantir uma perfeita interoperabilidade.
- 4.1.1.3 Deve estar licenciado para permitir o controle e gerenciamento centralizado através da solução de controladora wireless em nuvem por um período de no mínimo 60 (sessenta) meses;
- 4.1.1.4 Deve ser fornecido kit antifurto “Kensington security lock” ou equivalente com a finalidade de evitar o furto do equipamento.
- 4.1.1.5 Deve possibilitar a fixação do equipamento em teto e parede. Devem ser fornecidos todos os acessórios necessários para que possa ser feita a fixação, juntamente com kit antifurto.
- 4.1.1.6 Cada Ponto de Acesso WiFi deve ser entregue com 02 (dois) cabos UTP CAT6 de 1,5 metros.
- 4.1.1.7 Não deve haver restrição de licença que limite o número de usuários por Ponto de Acesso.

- 4.1.1.8 O modelo do equipamento ofertado deve possuir, na data da entrega da proposta, homologação junto à ANATEL com certificado disponível publicamente no endereço eletrônico desta agência, conforme a Resolução número 242 de 30 de novembro de 2000.
- 4.1.1.9 Deve ser acompanhado de todos os acessórios necessários para instalação, configuração e operação do equipamento, tais como: softwares, documentação técnica, acessórios de fixação, etc.
- 4.1.1.10 Deve ser fornecido com todas as licenças necessárias para o pleno funcionamento do ponto de acesso em conjunto com a solução de controladora wireless em nuvem, incluindo todos os recursos especificados neste Termo de Referência.

#### **4.1.2 Características Gerais**

- 4.1.2.1 Possuir no mínimo 01 (uma) porta Gigabit Ethernet (10/100/1000Base-T – IEEE 802.3, IEEE 802.3u e IEEE802.3ab) autosense, UTP RJ45.
- 4.1.2.2 Deve permitir ser alimentado através da tecnologia PoE IEEE 802.3af ou 802.3at utilizando a porta de switch na qual está conectado, através de dispositivo “power injector” e através de fonte de alimentação externa VAC.
- 4.1.2.3 Cada “Ponto de Acesso WiFi” deverá ser fornecido com fonte de alimentação VAC com seleção automática de tensão entre 110-230VAC e 60Hz e cabo de força padrão ABNT NBR 14136 compatível com o equipamento ofertado. Não será aceito a entrega de dispositivo power injector para atendimento deste item.
- 4.1.2.4 Deverá ser fornecida e instalada a versão mais recente do software interno do ponto de acesso WiFi.
- 4.1.2.5 Deve possuir captive portal web de autenticação do tipo splash page local ou em conjunto com a solução de controladora wireless em nuvem. Este portal web de autenticação deve permitir customização e suportar integração com servidor radius da FDE para autenticar os clientes WiFi com informações de usuário e senha.
- 4.1.2.6 Deve implementar, localmente ou em conjunto com a solução de controladora Wireless em nuvem, integração com Radius e LDAP da FDE para fins de autenticação dos clientes WiFi.
- 4.1.2.7 Deve implementar, localmente ou em conjunto com a solução de controladora Wireless em nuvem, Security Assertion Markup Language (SAML), agindo como autenticador de um Provedor de Serviços (Service Provider - SP) solicitando informações de identidade de usuários a Provedores de Identidade (Identity Providers - IDP's) de terceiros.

- 4.1.2.8 Deve implementar recursos de filtro de aplicação para reconhecimento e bloqueio de conteúdos relacionados a jogos, compartilhamento de arquivos, redes sociais, entre outros. Caso este recurso necessite de licença, a mesma deve ser fornecida pelo mesmo período de tempo coberto pela garantia solicitada neste termo de referência.
- 4.1.2.9 Deve implementar a visualização/identificação e marcação das aplicações para permitir o bloqueio ou priorização.
- 4.1.2.10 Deve implementar recursos de firewall stateful.
- 4.1.2.11 Deve permitir a definição de endereços MAC para controle de acesso a rede WiFi.
- 4.1.2.12 Deve permitir a conexão de, no mínimo, 250 dispositivos simultâneos.
- 4.1.2.13 Deve localmente ou em conjuntos com a solução de controladora wireless em nuvem, implementar análise de espectro de RF em 2.4GHz e 5gHZ para identificação de outros pontos de acesso intrusos e não autorizados (rogues), além de interferências no canal habilitado no ponto de acesso e nos demais canais configurados na rede WiFi. A análise de espectro deve ser realizada de forma simultânea ao atendimento dos clientes do ponto de acesso, sem que estes sejam desconectados.
- 4.1.2.14 Deve localmente ou em conjunto com a solução de controladora wireless em nuvem, realizar o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar o tamanho da célula de RF. Ajustar automaticamente os canais 802.11 e realizar a detecção de interferências e reajustar os parâmetros de Rádio Frequência visando evitar problemas de cobertura e performance.
- 4.1.2.15 Deve permitir operação simultânea nos padrões IEEE 802.11b/g/n, na faixa de 2,4 GHz, e 802.11a/n/ac, na faixa de 5 GHz, através de rádios independentes (dual radio), com padrão de irradiação omnidirecional.
- 4.1.2.16 Deve implementar a tecnologia 802.11ac Wave 2 MU-MIMO (Multi-User, Multiple Input, Multiple Output).
- 4.1.2.17 Deve possuir certificação WiFi Alliance para operar nos padrões IEEE 802.11a/b/g/n/ac.
- 4.1.2.18 Deve implementar para 2.4GHz, no mínimo, MIMO (Multiple-Input and Multiple-Output) 2x2 com 2 fluxos espaciais;
- 4.1.2.19 Deve implementar para 5GHz, no mínimo, MIMO (Multiple-Input and Multiple-Output) 2x2 com 2 fluxos espaciais em SU-MIMO (Single User MIMO) e 2 fluxos espaciais em MU-MIMO (Multi-User MIMO).
- 4.1.2.20 Deve possuir antenas internas integradas (embutidas) com ganho de, no mínimo, 3.8 dBi para 2,4 GHz e 3.8 dBi para 5 GHz.

- 4.1.2.21 Deve implementar High-Throughput (HT): Canais de 20MHz, 40MHz para IEEE 802.11N e VHT20, VHT40, VHT80 para IEEE 802.11ac.
- 4.1.2.22 Deve implementar maximal-ratio combining (MRC) e Beamforming.
- 4.1.2.23 Deve Operar com DFS e OFDM.
- 4.1.2.24 Deve possuir suporte a CSD ou CDD.
- 4.1.2.25 Deve implementar protocolo CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance).
- 4.1.2.26 Ser compatível com os padrões WMM e 802.1p para priorização de tráfego.
- 4.1.2.27 Deve possuir potência máxima de transmissão, por rádio, de pelo menos 18dBm em 2,4 GHz e 18 dBm em 5 GHz.
- 4.1.2.28 Deve possuir capacidade para operação em modo "repetidor", permitindo a comunicação entre pontos de acesso WiFi sem a necessidade de cabeamento adicional permitindo desta forma o atendimento de usuários em locais isolados da localidade.
- 4.1.2.29 Deve possuir cliente DHCP, para configuração automática do endereço IP.
- 4.1.2.30 Deve permitir a conexão à rede de usuários em IPv4, IPv6 e suportar dual-stack (clientes IPv4 e IPv6 no mesmo ponto de acesso WiFi).
- 4.1.2.31 Deve ser gerenciável no mínimo através do protocolo SNMP versão 2.
- 4.1.2.32 Deve possuir a capacidade de criação de no mínimo 8 (oito) SSIDs.
- 4.1.2.33 Permitir habilitar e desabilitar a divulgação do SSID.
- 4.1.2.34 Deve permitir configurar o SSID para trabalhar nos modos NAT e BRIDGE. No modo NAT, o access point deverá distribuir IPs via DHCP para os clientes WiFi, que ao efetuarem alguma navegação, terão os seus IPs traduzidos para o endereço IP adquirido pelo ponto de acesso através da rede cabeada. No modo brige, o ponto de acesso fará uma ponte entre a rede local e a rede WiFi, permitindo que os clientes WiFi adquiram endereçamento IP via DHCP da própria rede local onde o ponto de acesso for instalado.
- 4.1.2.35 Deve possuir no mínimo 01 (um) LED indicativo do seu estado de operação.
- 4.1.2.36 O software interno e os arquivos de configuração devem ser armazenados em memória não-volátil, permitindo a sua atualização via solução de controladora wireless em nuvem.

- 4.1.2.37 Permitir o uso do protocolo de autenticação IEEE 802.1X para no mínimo EAP-TLS e EAP-PEAP/MSCHAPV2
- 4.1.2.38 Deve ser compatível com WPA (Wi-Fi Protected Access com algoritmo de criptografia TKIP e Message Integrity Check – MIC).
- 4.1.2.39 Deve implementar WPA2 com AES.
- 4.1.2.40 Deve ser compatível com o padrão IEEE 802.11i.
- 4.1.2.41 Deve permitir a implantação de VLANs segundo o padrão IEEE 802.1Q, permitindo a configuração de no mínimo 8 (oito) VLANs.
- 4.1.2.42 Deve implementar a técnica de direcionamento de banda, permitindo que clientes com suporte a faixa de frequência de 5 GHz se conectem aos Pontos de Acesso utilizando, preferencialmente, a faixa de 5 GHz.
- 4.1.2.43 Deve implementar o protocolo NTP (Network Time Protocol) ou o protocolo SNTP (Simple Network Time Protocol) em modo cliente.
- 4.1.2.44 Deve implementar o envio de eventos por meio do protocolo Syslog.
- 4.1.2.45 Deve implementar controle de limite de uso de banda por SSID e por cliente.
- 4.1.2.46 Deve, juntamente com a solução de Controladora Wireless em nuvem descrita neste anexo, detectar, classificar e gerar alarmes de interferências WiFi provenientes de dispositivos padrão IEEE 802.11.
- 4.1.2.47 Deve realizar o bloqueio da comunicação entre usuários que compartilhem um mesmo SSID, permitindo o isolamento dos usuários.
- 4.1.2.48 Deve implementar o controle de tráfego de broadcast evitando a degradação do serviço devido a propagação deste tipo de tráfego.
- 4.1.2.49 Deve implementar Wireless IDS para identificar ataques de RF como Denial Of Service, Flood Attack, Mapeamento de rede, entre outros.
- 4.1.2.50 Deve implementar detecção e contenção de rogue APs e de redes AD-Hoc sem desconectar os clientes WiFi IEEE 802.11 associados ao ponto de acesso.

### **4.1.3 Funcionalidades da solução de Controladora wireless em nuvem**

- 4.1.3.1 Deve ser uma plataforma em nuvem proprietária, responsável pelas seguintes funções na rede sem fio: administração, configuração e gerenciamento completo centralizado dos pontos de acesso WiFi (especificados neste anexo), funções de segurança para acesso, funções de segurança para tráfego de dados e controle, funções de



gerenciamento de RF (Rádio Frequência), funções de gerenciamento de usuários e funções de gerenciamento de dispositivos de usuários.

- 4.1.3.2 A solução de Controladora Wireless em Nuvem não deve ter restrição de licença que limite o número de Ponto de Acesso a ser controlado por ela, sendo escalável para gerenciar no mínimo 20.000 (vinte mil) pontos de acesso.
- 4.1.3.3 Deve disponibilizar uma Console de Gerenciamento Web acessível através de protocolo Criptografado, compatível com os principais browsers do mercado (Internet Explorer, Firefox e Chrome), permitindo também acesso a Console através de dispositivos móveis com sistema operacional IOS e Android;
- 4.1.3.4 Deve permitir habilitar e desabilitar os SSID's de forma automática e com agendamento periódico.
- 4.1.3.5 Deve realizar procedimentos automáticos de configuração, correção e aperfeiçoamento da cobertura e disponibilidade dos pontos de acesso.
- 4.1.3.6 Deve possuir ferramenta de gerenciamento para múltiplas localidades integrada;
- 4.1.3.7 Deve realizar otimização de radiofrequência, monitoramento e alertas.
- 4.1.3.8 Deve realizar o upgrade de softwares dos pontos de acesso WiFi.
- 4.1.3.9 Deve empregar criptografia de dados TLS ou SSL no canal de comunicação com os pontos de acesso WiFi.
- 4.1.3.10 Deve disponibilizar pelo menos 03 (três) níveis de acesso à Console de Gerenciamento Web, sendo:
  - 4.1.3.10.1 Administrador: acesso de leitura e escrita às configurações para o gerenciamento do sistema;
  - 4.1.3.10.2 Operador: acesso de apenas leitura às configurações para a monitoria, sem permissão para alterar configurações;
  - 4.1.3.10.3 Organizador de Visitantes: acesso e permissão exclusiva para criação de usuários temporários e visitantes para acesso a rede WiFi.
- 4.1.3.11 Deve permitir a criação de múltiplas redes distintas e segregadas, mas administradas na mesma console, permitindo assim a segmentação e agrupamento de Access Points que tenham objetivos comuns, permitindo uma melhor organização do ambiente de equipamentos administrados.
- 4.1.3.12 Deve permitir a criação de contas de usuários para acesso a rede WiFi. Estes usuários devem ficar armazenados na própria solução de controladora Wireless em nuvem.

- 4.1.3.13 Deve implementar recursos que permitam mecanismo de autenticação através de portal Web customizável (captive portal customizável) para clientes visitantes, com usuário e senha. Este mecanismo deve permitir ainda que o cliente visitante crie a sua própria conta de usuário, cuja validação deve ser realizada por meio de mensagem a ser enviada para o e-mail informado pelo cliente visitante durante o cadastro. No caso de a solução gerar um usuário e/ou senha automaticamente, estes dados devem ser informados ao visitante através de e-mail ou sms, ou captive portal. Todo o processo deve ser realizado sem a intervenção do administrador da solução que controla a solução wireless em nuvem.
- 4.1.3.14 Deve permitir a visualização de um conjunto de informações de análise dos Access Points que fazem parte da rede wireless, disponibilizando pelo menos as seguintes informações:
- 4.1.3.14.1 Relação dos Access Points conectados, disponibilizando no mínimo as informações de Nome, MAC Address, Modelo de equipamento e endereço IP;
  - 4.1.3.14.2 Quantidade de dispositivos conectados em cada Access Point, volume de dados utilizado, tempo de disponibilidade e SSIDs.
  - 4.1.3.14.3 Localização dos Access Points em planta baixa inserida no sistema, incorporando informações sobre os equipamentos gerenciados.
- 4.1.3.15 Deve permitir a visualização de um conjunto de informações dos dispositivos conectados à rede wireless, disponibilizando pelo menos os dados abaixo especificados:
- 4.1.3.15.1 Endereço IP, MAC Address, Hostname, Usuário;
  - 4.1.3.15.2 Sistema Operacional do dispositivo utilizado;
  - 4.1.3.15.3 Tempo de conexão;
  - 4.1.3.15.4 Informação do protocolo de conexão com a rede WiFi, SSID e Ponto de Acesso utilizados;
  - 4.1.3.15.5 Gráficos e Dados de utilização dos Usuários;
  - 4.1.3.15.6 Informações de destinos acessados;
- 4.1.3.16 Deve disponibilizar um formato de relatório sintético, com o resumo das principais informações estatísticas de utilização dos Access Point, como por exemplo: SSIDs mais usados, Usuários com maior consumo de dados, Aplicações mais utilizadas, Tipos de Dispositivos mais usados, Access Points mais utilizados, Volume Total de Banda e Quantidade Total de Usuários. Tal relatório ainda deve possibilitar ser enviado por e-mail, para usuários definidos pelo Administrador;

4.1.3.17 Deve possibilitar o agrupamento dos Access Point suportando a criação e o gerenciamento de grupos de Access Point simultâneos, permitindo assim criar nomenclaturas de organização como "Predio\_Central", "Primeiro\_Andar" entre outros.

4.1.3.18 Deve guardar os logs por um período de no mínimo 3 (três) meses.

#### **4.1.4 Garantia**

4.1.4.1 A garantia será em regime 8x5xNBD conforme descrito no item 6 (seis) deste projeto técnico.

## **5 Especificação Técnica dos Serviços de Instalação**

Este item corresponde à instalação e configuração do ponto de acesso WiFi nas Escolas.

### **5.1 Instalação e Configuração do Ponto de Acesso WiFi na Escola**

5.1.1 As atividades contempladas pelo serviço de instalação incluem: Planejamento, instalação física e configuração lógica do ponto de acesso e da controladora wireless em nuvem.

5.1.2 Deverá ser elaborado pela Contratada em conjunto com a FDE um plano de implantação contendo todo o detalhamento de implantação dos produtos nas unidades escolares.

5.1.3 O plano deverá contemplar o diagrama lógico da rede com todos os equipamentos envolvidos na solução e as configurações lógicas que serão realizadas em cada equipamento e software.

5.1.4 A contratada deverá criar e disponibilizar o cronograma das localidades que serão atendidas de acordo com a FDE.

5.1.5 O técnico da contratada deverá comparecer ao local, com a identificação da contratada, munido de documentação GPB (Guia de Passagem de Bens) relativa aos equipamentos entregues e relatório de instalação

impresso, que deverão ser preenchidos pelo técnico, assinados e carimbados por um responsável da unidade ao término do serviço. A escola ficará com uma cópia, a contratada com outra e a FDE com a última.

- 5.1.6 O Ponto de Acesso deverá ser configurado pela contratada conforme definições do plano de implantação acordado com a FDE no item 5.1.2.
- 5.1.7 O Ponto de Acesso deverá ser renomeado de acordo com o ambiente onde será instalado, conforme definição da FDE.
- 5.1.8 Antes da fixação, o técnico da contratada deverá fotografar os equipamentos que serão instalados, para controle dos equipamentos (número de série e mac address).
- 5.1.9 A contratada deverá instalar e energizar o Ponto de Acesso WiFi em local indicado pela FDE, utilizando o kit de instalação e kit antifurto, fixando o Ponto de Acesso WiFi no local determinado.
- 5.1.10 O técnico da Contratada deverá conectar o Ponto de Acesso ao ponto lógico indicado pela FDE. Após a fixação do AP com o kit de instalação e kit antifurto, o técnico deverá tirar fotos da instalação para finalizar o serviço. As fotos deverão ser encaminhadas para validação final da FDE.
- 5.1.11 Após o término da instalação, deverão ser efetuados testes para comprovação do pleno funcionamento dos equipamentos. Ao final do processo, a contratada deverá entrar em contato com a equipe da FDE para validação da instalação.
- 5.1.12 A FDE validará o serviço executado pela contratada, mediante contato telefônico do técnico ainda no local e após o recebimento dos relatórios e fotos para confirmação das instalações físicas.
- 5.1.13 A infraestrutura elétrica e cabeada será de responsabilidade da FDE.

## **6 Garantia**

A CONTRATADA deverá prover garantia para os equipamentos e softwares descritos neste projeto técnico, de forma uniforme para todos os equipamentos e serviços contratados, os quais deverão prover atendimento remoto e on-site por 48 meses, observando-se as seguintes características descritas neste item.

## 6.1 Características Gerais

- 6.1.1 A garantia deverá ser prestada de forma a atender todas as necessidades da FDE em manter o perfeito funcionamento de todos os equipamentos e softwares, objetos desta contratação.
- 6.1.2 Em não havendo possibilidade de reparo do equipamento, este deverá ser substituído por outro de igual configuração ou superior, sem ônus para a FDE, restaurando assim o pleno funcionamento do ambiente. Neste caso, o número de série e demais dados do novo equipamento deverão ser informados à FDE para controle e gerenciamento dos ativos.
- 6.1.3 Sempre que houver necessidade de manutenção externa, o transporte e o seguro dos equipamentos ocorrerão por conta da contratada e sem ônus para a FDE.
- 6.1.4 Ao visitar a unidade, a contratada deverá estar munida de documentos de identificação e relatório técnico impresso que deverá ser preenchido com letra legível, ao final do atendimento e assinada pelo acompanhante do serviço na unidade. Uma cópia ficará em poder da unidade e a outra com o técnico da contratada.
- 6.1.5 A contratada ao prestar manutenção deverá estar munida de todos os equipamentos e ferramentas necessárias para realizar os serviços de configuração e manutenção, descritos nestas especificações.
- 6.1.6 A Contratada deverá disponibilizar todas as atualizações dos softwares e firmwares dos equipamentos sem nenhum tipo de custo adicional para a FDE.
- 6.1.7 A Contratada deverá prover serviços de Teleatendimento e de Internet (correio ou Web) para que a FDE possa fazer abertura de chamados e acionar o serviço de garantia em horário comercial compreendido entre as 07hs e 20hs, de segunda à sexta-feira. Os serviços de manutenção deverão ser realizados pela CONTRATADA no horário comercial compreendido entre as 08hs e 18hs, de segunda à sexta-feira;
- 6.1.8 Os tempos máximos para atendimento e solução do problema por parte da CONTRATADA serão contados a partir da abertura do chamado técnico, que deverá ser efetuado pelo representante da FDE.
- 6.1.9 A garantia deverá ser disponibilizada pela CONTRATADA em regime 8x5x24h, conforme detalhamento abaixo:
  - 6.1.9.1 Tempo de Atendimento: Suporte técnico (08 horas por dia e 05 dias por semana em horário comercial) incluso a substituição avançada de peças, com um técnico de campo conforme solicitação da FDE, entregue no próximo dia útil da determinação de que se faz necessária a

---

substituição de quaisquer peças e/ou equipamentos (8 horas por dia e 05 dias por semana em horário comercial).

6.1.9.2 Tempo de Solução: Os chamados, seja com ou sem substituição de peças, devem ser solucionados até o final do dia útil subsequente ao dia de sua abertura.

6.1.10 Quando houver a necessidade de substituição de qualquer um dos equipamentos ou softwares objeto desta contratação, a Contratada deverá fornecer equipamento com características iguais ou superiores ao equipamento original, mediante aprovação por parte da unidade gestora do contrato.

6.1.11 A Contratada deverá ainda complementar os serviços objeto desta contratação com os seguintes itens providos por meio de suporte direto junto ao fabricante:

6.1.11.1 Ter acesso ao fabricante para o escalonamento de chamados técnicos, caso não tenha sido possível oferecer solução por meios próprios.

6.1.11.2 Licenciar ao CONTRATANTE as seguintes funcionalidades junto ao fabricante:

6.1.11.2.1 Acesso direto ao seu centro de assistência técnica;

6.1.11.2.2 Acesso aos novos releases de software;

6.1.11.2.3 Acesso à sua base de conhecimento, provendo informações, assistência e orientação para:

1. Instalação;
2. Desinstalação;
3. Diagnósticos, avaliações e resolução de problemas;
4. Características dos produtos em geral;
5. Demais atividades relacionadas à correta operação e funcionamento dos equipamentos e softwares.

## **7 Capacitação**

Fornecimento de serviço de capacitação em conceitos e funcionamento de redes WiFi, gerenciamento, configuração e resolução de problemas em Redes WiFi para os pontos de acesso WiFi e solução de controladora Wireless em nuvem.

### **7.1 Características Gerais**

7.1.1 Local a ser ministrado: Dependências da Contratante.

- 7.1.2 Quantidade de participantes.
- 7.1.3 O treinamento deve incluir apostilas, manuais, exercícios práticos e laboratório para configuração da solução de rede WiFi ofertada.
- 7.1.4 A duração mínima deste treinamento não deve ser inferior a 40 horas.
- 7.1.5 Deverão ser fornecidos certificados de participação aos alunos contendo nome do curso, empresa responsável, data de realização e carga horária, no mínimo.

## **7.2 Capacitação Técnica**

- 7.2.1 Descrever detalhadamente técnicas de modulação e propagação e como estas são usadas com diferentes tipos de antenas.
- 7.2.2 Instalar e configurar Pontos de Acesso WiFi.
- 7.2.3 Configurar basicamente uma rede WiFi.
- 7.2.4 Configurar funcionalidades avançadas de WiFi através da solução de controladora wireless em nuvem incluindo captive portal e autenticação 802.1x.
- 7.2.5 Implementar soluções de gerenciamento e controle da rede WiFi.
- 7.2.6 Conhecer conceitos e métodos para aplicação de segurança em um ambiente WiFi.
- 7.2.7 Conhecer funcionalidades avançadas para melhor utilização dos equipamentos e software adquiridos.
- 7.2.8 Entender detalhadamente as características, funcionalidades e benefícios da arquitetura de uma rede sem fio baseada em controladora wireless em nuvem.
- 7.2.9 Instalar e configurar detalhadamente redes wireless usando a plataforma de controladora wireless em nuvem, incluindo funcionalidades de visibilidade e monitoramento.
- 7.2.10 Realizar o troubleshooting nos aspectos do hardware e software e manter redes wireless operando.
- 7.2.11 Adicionar aplicações avançadas às redes wireless – voz e vídeo.
- 7.2.12 Aplicação de QOS;
- 7.2.13 Garantir a segurança de redes wireless na solução adquirida.

## **8 Homologação**

A vencedora do certame deverá fornecer para análise amostra do item 4.1 em consonância com as especificações técnicas descritas no Anexo II do Edital, em até 03 (três) dias úteis, a partir da data da assinatura do Contrato, na Gerência de Gestão de Recursos e Serviços, na Av. São Luis, 99 – 16º andar – Centro – São Paulo/Capital. A FDE terá um prazo de 7 (sete) dias úteis para homologar o produto. Na hipótese da amostra apresentar ressalvas na análise realizada pela Comissão de Análise Técnica desta Fundação, a licitante se comprometerá a entregar no prazo de 03 (três) dias úteis nova amostra para análise, sanando todas as ressalvas apresentadas. A FDE realizará somente duas etapas de homologação, sendo que a segunda deverá seguir os mesmos prazos da primeira homologação. Caso o produto não seja homologado na segunda etapa, a Contratada será desclassificada.