ANEXO I

TERMO DE REFERÊNCIA
DESCRIÇÃO DO AMBIENTE DE TIC DA PMSP

A PRODAM é uma empresa de economia mista, criada em 1971, com a finalidade de contribuir para a organização administrativa da Prefeitura da Cidade de São Paulo. Consolidou-se ao longo de sua história como instrumento de gestão da mais alta importância. Apóia a prefeitura na elaboração das políticas de informação e de informática da Cidade, assim como atua na modernização dos órgãos e entidades municipais, oferecendo serviços nas áreas de Tecnologia da Informação e de Comunicação (TIC), viabilizando um atendimento de qualidade à população e contribuindo para o desenvolvimento social e econômico.

Magnitude de atuação da Prefeitura Municipal de São Paulo

População Brasileira 191,5 milhões de Habitantes

Estados		**Cidades**	
São Paulo	41,4 milhões	São Paulo	11,04 milhões
Minas	20 milhões	Rio de Janeiro	6,19 milhões
Rio de Janeiro	16 milhões	Salvador	3,00 milhões
		Brasília	2,61 milhões
		Fortaleza	2,51 milhões

(Fonte IBGE – 14/08/2009)

A prefeitura atende uma população de cerca de 20 milhões de habitantes, em sua área metropolitana, que usam parte dos serviços essenciais da cidade de São Paulo, e, com o objetivo de facilitar a gestão administrativa, a cidade foi descentralizada em 31 sub prefeituras e diversos núcleos regionais de atuação na área de saúde e educação.

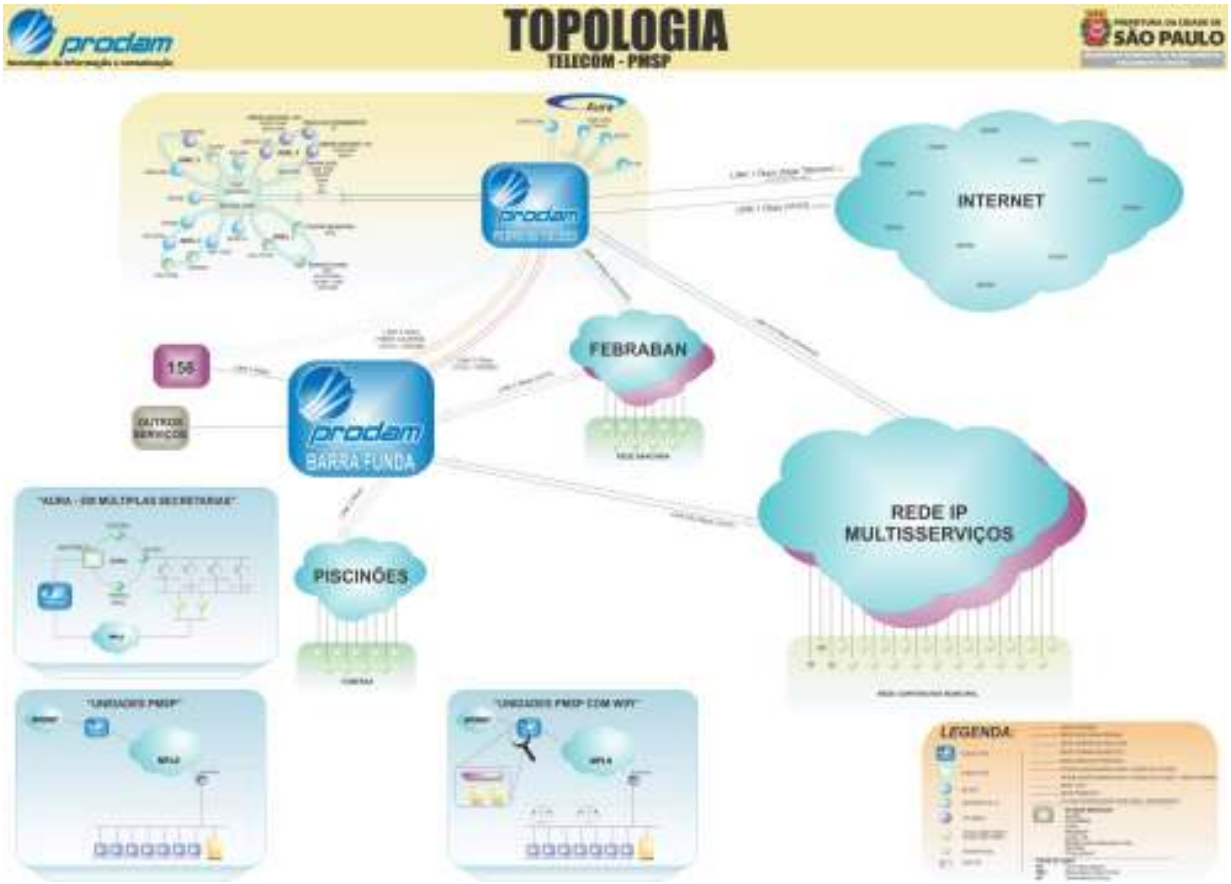
A rede municipal de ensino da cidade de São Paulo supera a um milhão de crianças e jovens. Somados aos pais e familiares, envolve quase cinco milhões de pessoas, ultrapassando, e muito, a população da maioria das capitais brasileiras. Com mais de 78 mil funcionários, entre educadores e pessoal de apoio, a rede de ensino tem 1.417 escolas espalhadas por todos os cantos da cidade, administradas diretamente pela Secretaria Municipal de Educação. Acrescentam-se e elas as 300 creches indiretas, operadas por entidades conveniadas, e os 649 convênios assinados com creches particulares e entidades alfabetizadoras

Na área de saúde, são mais de 877 estabelecimentos, prestando diversos serviços de atendimento médico e laboratorial ao cidadão.

Como pode ser visto, a cidade de São Paulo é altamente complexa, com 11,04 milhões de habitantes, ocupando uma área de 1.523 km².

Para garantir o perfeito funcionamento dos serviços públicos em benefício da sociedade, foi construída uma ampla infraestrutura de tecnologia de informação e comunicação, que não para de crescer. Manter essa infraestrutura atualizada e disponível requer competência e seriedade de todos os colaboradores diretos e indiretos, que estão envolvidos no ciclo de governança corporativa da cidade de São Paulo.

Diagrama Técnico da Rede de Comunicação da PMSP



A rede de comunicação da PMSP possui uma infraestrutura própria, baseada em anéis de fibra ótica com aproximadamente 74 Km de extensão, atendendo as principais secretarias localizadas na zona central da cidade. Possuímos ainda uma rede baseada em tecnologia MPLS, com um concentrador de 1 Gbps, interligando mais de 3.100 unidades da prefeitura, distribuídas pela cidade de São Paulo. Um backbone internet com dupla abordagem de operadoras de 1 Gbps, atualmente utilizando 350 Mbps, provê ao cidadão, acesso direto aos serviços públicos através do portal da prefeitura. São milhões de acessos diários, agilizando o atendimento público e reduzindo filas nos postos de atendimento.

A rede interna dos órgãos da prefeitura possui aproximadamente 8.000 switchs de 24 portas, atendendo mais de 90 mil estações de trabalho, atuando nas áreas de saúde, educação, gestão administrativa e financeira da cidade, além de diversos outros serviços públicos.

O serviço de correio eletrônico provê 55.000 caixas-postais e apresenta um tráfego de 1.2 milhões de mensagens enviadas e recebidas por dia, através da internet, sem considerar o tráfego interno.

Todos esses serviços são concentrados no datacenter principal e de contingência da Prodam, que possuem capacidade de processar e armazenar um grande volume de dados e informações. São mais de 700 servidores em diversas plataformas tecnológicas e cerca de 60 TB de armazenamento em disco, além de contar com uma moderna infraestrutura, fornecendo aos seus clientes confiabilidade, integridade, disponibilidade, flexibilidade e segurança na prestação de seus serviços.

ÍNDICE

1. DESCRIÇÃO GERAL DO PROJETO BÁSICO DE CONTRATAÇÃO DE EQUIPAMENTOS DE REDES WIRELESS PARA O MUNICÍPIO DE SÃO PAULO COM SUPORTE, INSTALAÇÃO E MANUTENÇÃO.

1.1. Sobre a propriedade dos equipamentos:

1.1.1. Todos os equipamentos contidos no edital serão de propriedade das secretarias e órgãos que aderirem e contratarem a Ata de Registro de Preços, excetuando as controllers e os softwares de gerencia que serão exclusivamente de propriedade da PRODAM.

1.2. Conectividade:

1.2.1. As conexões dos Access Points contidos nesta ARP (Ata de Registro de Preços) necessariamente deverão ser gerenciados pelas controllers fornecidas por este Termo de Referencia e hospedadas e mantidas pela PRODAM.

1.3. Compatibilidade

1.3.1. Todos os equipamentos do item I deste termo de referência e do item A e B do "Anexo A" devem ser do mesmo fabricante. Caso os Access Points operem com todas as características técnicas utilizando processamento colaborativo, com gerencia centralizada, dispensando a necessidade de uma ***Appliance***/controladora, os equipamentos do item I deste termo de referência deverão ser do mesmo fabricante do gerenciamento centralizado, descrito no item B do "anexo A".

1.4. Certificações

1.4.1. Equipamentos da Solução Wireless

1.4.1.1. Os equipamentos na data da entrega da proposta devem estar homologados pela ANATEL (Agência Nacional de Telecomunicações);

1.4.1.2. Os equipamentos na data da entrega da proposta devem possuir as certificações Wi-Fi Alliance (Wi-Fi Certified), WMM (Wi-Fi Multimedia Quality);

1.4.2. Equipamentos de distribuição Switches

1.4.2.1. Os equipamentos na data da entrega da proposta devem estar homologados pela ANATEL (Agência Nacional de Telecomunicações);

1.5. Gerenciamento da rede:

1.5.1. A contratada deverá disponibilizar exclusivamente para a PRODAM Ferramenta de gerenciamento da solução, sendo ela uma única ou um conjunto de ferramentas deste que devidamente integrada.
1.5.2. A exclusividade no gerenciamento da plataforma e necessário para manter o controle e segurança na rede PMSP.

1.6. Serviços De Manutenção, Suporte Técnico e Garantia.

1.6.1. A CONTRATADA deve fornecer suporte técnico remoto na língua Portuguesa para toda a solução tanto hardware quanto software durante o período de vigência da garantia, assegurando atendimento a incidente de produção.
1.6.2. Regime de atendimento dos chamados de suporte técnico deverá ser de 24 horas por dia, 7 dias por semana, 365 dias do ano.
1.6.3. Abertura de chamados: Site Web, telefone e/ou email. Este serviço deverá estar disponível 24 horas por dia, 7 dias por semana.
1.6.4. Equipamentos contemplados:
1.6.4.1. Controladoras deste Termo de Referência
1.6.4.2. Access Points deste Termo de Referência
1.6.4.3. Switches deste Termo de referência
1.6.5. Tempo de retorno referente ao 1º contato técnico no chamado com o efetivo início do atendimento técnico:
1.6.5.1. Até 2 horas a contar da hora de abertura do chamado fornecendo orientações para diagnóstico de problemas e ajuda na interpretação de traces, dumps e logs, além de escalonar caso necessário a central de suporte do fabricante de forma a envolver no atendimento do chamado a engenharia de produto. O atendimento deverá ser promovido por telefone e/ou acesso remoto, sendo que caso seja necessário deverá ser complementado com atendimento on-site. O tempo de chegada ao site da CONTRATANTE do técnico da CONTRATADA deve ser de até 2 horas após a abertura do chamado.
1.6.6. Os atendimentos cujas interações de correções necessitarem de continuidade após o horário comercial, deverão ter suas continuidades garantidas pela CONTRATADA.

1.6.7. Adicionalmente, a CONTRATADA deve fornecer o suporte técnico do fabricante vinculado aos equipamentos constante neste descritivo técnico. O suporte técnico do fabricante deve ser fornecido conforme os seguintes requisitos:

1.6.7.1. Suporte técnico de nível 2 (substituição de equipamentos em campo) e 3(suporte para problemas construtivos) do fabricante a todos os itens ofertados, de forma a garantir o cumprimento de todos os requisitos abaixo.

1.6.7.1.1. Disponibilizar acesso aos funcionários da CONTRATANTE para que possam acessar os softwares e ferramentas diretamente com o fabricante.

1.6.7.1.2. Possuir suporte técnico remoto para todos os itens ofertados durante o período de vigência da garantia, assegurando atendimento a incidentes da produção:

1.6.7.2. Regime de atendimento dos chamados de suporte técnico deve ser de 24 horas por dia, 7 dias por semana.

1.6.7.3. Abertura de chamados: Site Web, Telefone e/ou Email. Este serviço deverá estar disponível 24 horas por dia, 7 dias por semana com geração de número de protocolo de atendimento, o qual só poderá ser fechado após confirmação com técnicos da PRODAM.

1.6.8. Modalidade do atendimento conforme a severidade:

1.6.8.1. **Severidade Alta** (equipamento está indisponível): Atendimento remoto de consultor especializado, com tempo de retorno referente ao 1º contato técnico no chamado e com o efetivo início do atendimento técnico em até 1 hora após a abertura do chamado.

1.6.8.2. **Severidade Média** (equipamento apresenta indisponibilidade parcial ou lentidão): Atendimento remoto de consultor especializado, com tempo de retorno referente ao 1º contato técnico no chamado e com o efetivo início do atendimento técnico no próximo dia útil, em horário comercial, após a abertura do chamado.

1.6.8.3. **Severidade Baixa** (equipamento apresenta lentidão ou mensagens de alerta / erro, mas o serviço está disponível): Atendimento remoto de consultor especializado, com tempo de retorno referente ao 1º contato técnico no chamado e com o efetivo início do atendimento técnico nos próximos 2 dias uteis, em horário comercial, após a abertura do chamado.

1.6.9. O suporte técnico deverá fornecer orientações para diagnóstico de problemas e ajuda na interpretação de traces, dumps e logs sempre acionando a engenharia de produto para os chamados de severidade **Alta** (nível 3) e **Média** (nível 2).

1.6.10. Os atendimentos cujas interações de correções necessitarem de continuidade após o horário comercial, deverão ter suas continuidades garantidas.

1.6.11. O suporte técnico deverá prover informações sobre correções, ou a própria correção. Nos casos de defeitos não conhecidos, as documentações recebidas da instalação (tais como:

traces, dumps e logs) deverão ser encaminhadas aos laboratórios dos produtos a fim de que sejam fornecidas as devidas soluções.

1.6.12. A garantia de toda a solução ofertados é de no mínimo **36 (trinta e seis) meses** para todos os equipamentos, softwares, módulos e todos os itens da solução, a ser provida diretamente pelo fabricante.

1.6.13. Todos os equipamentos constantes neste descritivo técnico deverão ter acesso direto ao fabricante para atualização dos softwares instalados e fornecimento de novas versões de software, por necessidade de correção de problemas ou por implementação de novos releases.

1.6.14. Em caso de defeito no equipamento, onde o diagnóstico aponte para problemas com o hardware:

1.6.14.1. Caso seja detectada a necessidade de troca de todo o equipamento, o fabricante deverá prover, através de seus serviços formais, o equipamento substituto com hardware de mesmo modelo ou superior.

1.6.14.2. A CONTRATADA deverá promover toda a logística de entrega do equipamento substituto nas dependências onde se encontra o equipamento com defeito e a retirada do mesmo, sem custo para a CONTRATANTE.

1.6.14.3. A CONTRATADA deve garantir a conclusão dessa operação de substituição em até, no máximo, **2 dias úteis**, a contar da data de abertura do chamado.

1.6.14.4. A CONTRATADA deve garantir também a instalação física e reconfiguração plena do novo equipamento, colocando o mesmo em operação normal, instalando a mesma configuração originalmente existente no equipamento que apresentou defeito. Para esta operacionalização plena após uma manutenção de hardware, a CONTRATANTE deverá fornecer os backups das configurações lógicas que estavam em funcionamento no equipamento afetado para que sejam aplicados no equipamento substituto.

1.6.15. Atualizações de software:

1.6.15.1. Todos os equipamentos envolvidos nesta garantia deverão possuir atualização de software/firmware durante o período contratual.

1.6.16. Penalidades

1.6.16.1. Além das sanções legais da lei 8666/93, a contratada estará sujeita ao pagamento de multa de 10% (dez por cento) do valor mensal do contrato, se ao longo do mês houver descumprimento de:

-01 Ocorrência de severidade alta
-02 Ocorrências de severidade média
-04 Ocorrências de severidade baixa

1.6.16.2. A reincidência por 03 meses consecutivos, ou 05 eventos ao longo de 12 meses facultarão à contratante rescindir o contrato, cabendo à contratada o ônus de desinstalação dos equipamentos, bem como pagamento de multa prevista em lei.

1.7. Autenticação:

1.7.1. O sistema de autenticação da solução utilizará o “captive portal” da PRODAM (composto de site de controle de usuários e RADIUS de acesso público) para munícipes e a solução RADIUS corporativa (sob IEEE 802.1X);

1.8. Relatórios e logs:

1.8.1. A CONTRATADA deverá disponibilizar, através das ferramentas fornecidas, os seguintes relatórios:

- Utilização por antena;
- Utilização por equipamento (em kbps);
- Utilização por usuário (em kbps);
- Invasores (rogue AP);
- Frequências ofensoras (Fornos de micro-ondas, Bluetooth, Telefones sem fio);
- Conexões Ad-Hod indevidas;
- Acesso aos equipamentos;
- Alarmes de equipamentos;

1.9. Operação:

1.9.1. Toda a operação das redes wireless deve seguir os padrões e homologação da ANATEL;

1.9.2. Deve suportar as taxas de transmissão: 3 Mbit/s (Salto em frequência), 11 Mbit/s (sequência direta), 54 Mbit/s (OFDM 802.11a e 802.11g), 144 Mbit/s (OFDM 802.11n 20 MHz), 300 Mbit/s (OFDM 802.11n 40 MHz), 390 Mbit/s (OFDM 802.11ac 80 MHz)

1.9.3. e 866,7 Mbit/s (OFDM 802.11ac 160 MHz).

1.10. Infraestrutura:

1.10.1. Equipamentos e materiais mínimos envolvidos na prestação do serviço:

- Access Points;
- Controladoras;
- Servidores de gerenciamento;
- Switches PoE;

1.10.2. **Instalação**:

1.10.2.1. As atividades contempladas pelo serviço de instalação incluem: Planejamento, instalação física e configuração dos seguintes itens:

1.10.2.1.1. Access Points deste termo de referencia

1.10.2.1.2. Switches deste termo de referencia

1.10.2.1.3. Controladoras deste termo de referencia

1.10.2.1.4. Acessórios

1.10.2.2. A contratada deverá fornecer o “Plano de Instalação e Configuração” dos equipamentos;

1.10.2.3. 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, em conformidade com o **site survey** entregue pela contratante.

1.10.2.4. Os equipamentos deverão ser instalados em locais definidos nos **site survey** realizados nas localidades, de responsabilidade da contratante;

1.10.2.5. A contratada deverá efetuar a configuração lógica definida no plano de instalação e configuração. Após a configuração, deverão ser efetuados testes para comprovação do pleno funcionamento dos equipamentos;

1.10.2.6. Toda a infraestrutura necessária para o atendimento de TODOS os itens deste Termo de Referencia é de responsabilidade da CONTRATANTE ou pressuposta conforme **site survey** entregue.

1.10.2.7. Parte Elétrica;

1.10.2.7.1. A responsabilidade de toda a parte elétrica, do quadro elétrico até os equipamentos instalados, será da CONTRATANTE ou pressuposta;

2. ESPECIFICAÇÃO TÉCNICA

Item I:

Access Points, licença e instalação.

Para o pleno atendimento dos Access points, as controladoras deverão ser fornecidas, sem custo, e em redundância 1+N, sendo instaladas na PRODAM conforme especificado no Anexo II, atendendo o total de access points descritos nos itens I.a e I.b ou que operem com todas as características técnicas, utilizando processamento colaborativo com gerencia centralizada, dispensando assim a necessidade de controladoras;

2.1. I.A – Access Point Indoor 802.11 a/b/g/n/ac nas frequências de 2.4GHz e 5GHz, Quantidade _____

2.1.1. Devem ser fornecidos equipamentos para ambiente interno suportando as arquiteturas abaixo, com a instalação, cabos, softwares e demais componentes necessários ao seu perfeito funcionamento e integração à solução ofertada, deve ter no mínimo as seguintes características técnicas:

2.1.2. Certificações:

2.1.2.1. O equipamento na data de entrega da proposta deve estar homologado pela ANATEL (Agência Nacional de Telecomunicações);

2.1.2.2. O equipamento na data de entrega da proposta deve possuir as certificações Wi-Fi Alliance (Wi-Fi Certified), WMM (Wi-Fi Multimedia Quality);

2.1.3. Operação:

2.1.3.1. Deve funcionar no modo gerenciado por Controlador Wireless LAN ou com processamento colaborativo, conforme descrito no item 1 do Anexo A deste Termo de Referência;

2.1.3.2. Deve ser capaz de operar em malha de rede “Mesh”, ou equivalente;

2.1.3.3. Caso seja utilizado *trunk* por rádio, este deve operar em frequências distintas às do tráfego de dados da rede;

2.1.3.4. Deve atender ao padrão MIMO 3x3;

2.1.3.5. Deve possuir duplo rádio permitindo operação simultânea nas faixas de 2;4 GHZ e 5 GHz

2.1.3.6. Deve permitir redes locais, em que o tráfego dos APs não é encaminhado para a controladora e/ou gerenciamento, e redes centralizadas, em que todo tráfego de rede deve ser encaminhado para a controladora e/ou gerenciamento.

2.1.4. Licenciamento:

2.1.4.1. Deve acompanhar uma licença descrita no item Operação;

2.1.5. Arquitetura;

2.1.5.1. IEEE 802.11 a/b/g/n/ac (2.4GHz e 5GHz);

2.1.6. Segurança

2.1.6.1. Possuir trava de segurança padrão “Kensington Lock”;

2.1.6.2. WPA2, WPA, 802.11i;

2.1.6.3. AES, TKIP, 802.1X - EAP-MD5; EAP-FAST (Flexible Authentication via Secure Tunneling); EAP-GTC (EAP – Generic Token Card); PEAP-MSCHAPv2 (PEAP – Microsoft Challenge Authentication Protocol Version 2); EAP-TLS (EAP – Transport Layer Security);

2.1.6.4. Chave dinâmica por sessão e por usuário;

2.1.6.5. Criação de filtros de endereços MAC;

2.1.6.6. Criação de filtros por endereços IP;

2.1.6.7. Deve possuir Seleção de Frequência Dinâmica (DFS) para a frequência de 5 Ghz de acordo com o padrão IEEE 802.11h

2.1.6.8. Deve suportar captura de pacotes na interface wireless para diagnóstico

2.1.7. Gerenciamento;

2.1.7.1. SNMP v2c e v3;

2.1.7.2. Telnet ou SSH(IPSEC);

2.1.7.3. Web-management; ou CLI padrão;

2.1.7.4. Suporte à configuração do Access Point de modo que ele não faça broadcast do(s) SSID (identificador único) da rede WLAN;

2.1.7.5. Suporte à configuração individual de, no mínimo, 5 (cinco) SSID;

2.1.8. Qualidade de Serviço:

2.1.8.1. Implementação de VLAN segundo o padrão IEEE 802.1Q;

2.1.8.2. Implementação de Class of Service (CoS) segundo o padrão IEEE 802.1p;

2.1.8.3. Implementação de Quality of Service (QoS);

2.1.8.4. Suporte à configuração dos parâmetros wireless, gerenciamento das políticas de segurança, QoS e monitoração de RF (rádio frequência);

2.1.8.5. Implementação de mapeamento DSCP (Differentiated Services Code Point mapping);

2.1.8.6. Deve suportar a atualização automática de firmware através da controladorora

2.1.8.7. Deve suportar seleção automática de canais

2.1.8.8. Deve implementar Beamforming

2.1.9. Fonte AC:

2.1.9.1. Entrada: 100-240VAC;

2.1.10. Alimentação remota de energia;

2.1.10.1. Implementar IEEE 802.3af Power over Ethernet;

2.1.10.2. Fornecido com Power injector ;

2.1.11. Opções de Antena:

2.1.11.1. Mínimo uma antena omnidirecional interna ou externa de, no mínimo, 4 dBi para a frequência de 2,4GHz;

2.1.11.2. Mínimo uma antena omnidirecional interna ou externa de, no mínimo, 2 dBi para a frequência de 5GHz;

2.1.12. Interfaces:

2.1.12.1. 01 (uma) porta Ethernet (100/1000Base-TX – IEEE 802.3, IEEE 802.3u) autosense;

2.1.12.2. 01 (uma) interface de console para gerenciamento por linha de comando compatível com o padrão EIA/TIA-232, podendo utilizar o conector da porta Ethernet;

2.1.12.3. EIRP: O conjunto rádio com antenas deve proporcionar nível de sinal de pelo menos 30 dBm para todas modulações exigidas neste termo de referência.

2.1.12.4. A sensibilidade de recepção dos Access points deve ser de no mínimo de -75 dBm para todas modulações exigidas neste termo de referência.

2.2. I.B – Access Point Indoor IEEE 802.11 b/g/n na frequência de 2.4GHz, Quantidade ____

2.2.1. Devem ser fornecidos equipamentos para ambiente interno suportando as arquiteturas abaixo, com a instalação, cabos, softwares e demais componentes necessários ao seu perfeito funcionamento e integração a solução ofertada, deve ter no mínimo as seguintes características técnicas:

2.2.2. Certificações:

2.2.2.1. O equipamento na data de entrega da proposta deve estar homologado pela ANATEL (Agência Nacional de Telecomunicações);

2.2.2.2. O equipamento na data de entrega da proposta deve possuir as certificações Wi-Fi Alliance (Wi-Fi Certified), WMM (Wi-Fi Multimedia Quality);

2.2.3. Operação:

2.2.3.1. Deve funcionar no modo gerenciado por Controlador Wireless LAN ou com processamento colaborativo, conforme descrito no item 1 do Anexo A deste Termo de Referência;

2.2.3.2. Deve ser capaz de operar em malha de rede “Mesh” ou equivalente;

2.2.3.3. Caso seja utilizado *trunk* por rádio, este deve operar em frequências distintas às do tráfego de dados da rede;

2.2.3.4. Devem atender o padrão MIMO 2x2

2.2.3.5. Deve permitir redes locais, em que o tráfego dos APs não é encaminhado para a controladora e/ou gerenciamento, e redes centralizadas, em que todo tráfego de rede deve ser encaminhado para a controladora e/ou gerenciamento.

2.2.4. Licenciamento:

2.2.4.1. Deve acompanhar uma licença descrita no item Operação;

2.2.5. Arquitetura;

2.2.5.1. IEEE 802.11 b/g/n (2.4GHz);

2.2.6. Segurança

2.2.6.1. Possuir trava de segurança padrão “Kensington Lock”;

2.2.6.2. WPA2, WPA, 802.11i;

2.2.6.3. AES, TKIP, 802.1X - EAP-MD5; EAP-FAST (Flexible Authentication via Secure Tunneling); EAP-GTC (EAP – Generic Token Card); PEAP-MSCHAPv2 (PEAP – Microsoft Challenge Authentication Protocol Version 2); EAP-TLS (EAP – Transport Layer Security);

2.2.6.4. Chave dinâmica por sessão e por usuário;

2.2.6.5. Criação de filtros de endereços MAC;

2.2.6.6. Criação de filtros por endereços IP;

2.2.7. Gerenciamento;

2.2.7.1. SNMPv3;

2.2.7.2. Telnet ou SSH(IPSEC / TLS-SSL);

2.2.7.3. Web-management; ou CLI padrão;

2.2.7.4. Suporte à configuração do Access Point de modo que ele não faça broadcast do(s) SSID (identificador único) da rede WLAN;

2.2.7.5. Suporte à configuração individual de, no mínimo, 5 (cinco) SSID;

2.2.8. Qualidade de Serviço:

2.2.8.1. Implementação de VLAN segundo o padrão IEEE 802.1Q;

2.2.8.2. Implementação de Class of Service (CoS) segundo o padrão IEEE 802.1p;

2.2.8.3. Implementação de Quality of Service (QoS);

2.2.8.4. Suporte à configuração dos parâmetros wireless, gerenciamento das políticas de segurança, QoS e monitoração de RF (rádio frequência);

2.2.8.5. Implementação de mapeamento DSCP (Differentiated Services Code Point mapping);

2.2.9. Fonte AC:

2.2.9.1. Entrada: 100-240VAC;

2.2.10. Alimentação remota de energia;

2.2.10.1. Implementar IEEE 802.3af Power over Ethernet;

2.2.10.2. Fornecido com Power injector ;

2.2.11. Opções de Antena:

2.2.11.1. Mínimo uma antena omnidirecional interna ou externa de, no mínimo, 4 dBi para a frequência de 2,4GHz;

2.2.12. Interfaces:

2.2.12.1. 01 (uma) porta Ethernet (100/1000Base-TX – IEEE 802.3, IEEE 802.3u) autosense;

2.2.12.2. 01 (uma) interface de console para gerenciamento por linha de comando compatível com o padrão EIA/TIA-232, podendo utilizar o conector da porta Ethernet;

2.2.12.3. EIRP: O conjunto rádio e antenas deve proporcionar nível de sinal de pelo menos 30 dBm para todas modulações exigidas neste termo de referência.

2.2.12.4. A sensibilidade de recepção dos Access points deve ser de no mínimo de -75 dBm para todas modulações exigidas neste termo de referência.

2.2.12.5.

Item II:

Switches PoE e instalação, Quantidade ____

2.3. II.A – Switch de 24 portas

2.3.1. Deve ser montável em rack padrão EIA 19” (dezenove polegadas) e possuir kits completos para instalação;

2.3.2. Deve possuir, no mínimo, 24 (Vinte e quatro) portas 100/1000BaseTx em conectores do tipo RJ45 diretamente conectados ao equipamento, não sendo permitido o uso de conectores do tipo TELCO; Todas essas portas devem suportar o protocolo PoE (IEEE 802.3af);

2.3.3. Todas as 24 (vinte e quatro) portas devem suportar o protocolo PoE (IEEE 802.3af), disponibilizando 15 (quinze) watts de potência por porta;

2.3.4. 12 (doze) portas devem suportar o protocolo PoE+ (IEEE 802.3at), disponibilizando 30 (trinta) watts de potência por porta;

2.3.5. Deve possuir, no mínimo, 2 (duas) portas 10/100/1000Base-X, tipo SFP MiniGbic, compatível com conectores ópticos do tipo LC, Multimodo, populadas com MiniGbics novos e originais;

2.3.6. Deve permitir o empilhamento através de interfaces específicas e fixas no equipamento para este fim, sem a necessidade de módulos adicionais, e com uma capacidade de largura de banda de no mínimo 17(dezessete) Gbps bidirecionais;

2.3.7. Deve possuir fonte de alimentação interna ao equipamento, que opere com tensões de entrada entre 100 e 240VAC e suporte freqüência de 60 Hz nominais com tolerância de 5% para mais ou menos;

2.3.8. Deve suportar a instalação de fonte de energia redundante;

2.3.9. Deve permitir empilhar, no mínimo, 08 (oito) unidades e permitir o seu gerenciamento através de um único endereço IP;

2.3.10. Quando empilhado, deve permitir agregação de links (IEEE 802.3ad) entre quaisquer portas Gigabit, independentemente, das portas estarem em equipamentos diferentes da pilha;

2.3.11. Possuir capacidade de switching (Camada 2) de, no mínimo, 17(dezessete) Gbps;

2.3.12. Possuir performance mínima a 24 (vinte e quatro) Mpps;

2.3.13. Deve implementar funcionalidade de espelhamento de tráfego TX e RX, permitindo que as portas de origem e destino estejam em qualquer ponto da pilha;

2.3.14. Suportar, no mínimo, 8.000 (oito mil) endereços MAC;

2.3.15. Suportar gerenciamento via SNMP v1, v2c e v3.

2.3.16. Deve implementar IEEE 802.1p - (Classe de Serviços);

2.3.17. Deve implementar IEEE 802.1s - (Multiple Spanning Tree);

2.3.18. Deve implementar IEEE 802.1D - (Spanning Tree);

2.3.19. Deve implementar IEEE 802.1w – (Rapid Spanning Tree);

2.3.20. Deve implementar IEEE 802.3x – (Flow Control);

2.3.21. Deve implementar IEEE 802.1Q – (VLAN);

2.3.22. Deve implementar IEEE 802.3 ad (link aggregation), permitindo a criação de, no mínimo, 4 LAGs com 04 portas por LAG;

2.3.23. Deve implementar a RFC 3580 permitindo que um usuário autenticado por 802.1x seja automaticamente associado a sua respectiva VLAN;

2.3.24. Deve implementar IGMP v1, v2 e v3 e IGMP Snooping;

2.3.25. Deve implementar RADIUS client;

2.3.26. Deve ter suporte a Radius Authentication, Authorization e Accounting.

2.3.27. Deve implementar TFTP ou FTP client ;

2.3.28. Deve implementar Telnet;

2.3.29. Deve implemntar Syslog;

2.3.30. Deve implementar Command Line Interface – CLI;

2.3.31. Deve implementar Bridge MIB, RFC1493;

2.3.32. Deve implementar 4 (quatro) grupos RMON ;

2.3.33. Deve implementar MIB II, RFC1213;

2.3.34. Deve implementar RMON MIB, RFC 2819;

2.3.35. Deve implementar NTP ou SNTP;

2.3.36. Deve implementar Secured Shell (SSHv2);

2.3.37. Deve Possuir 1 (uma) porta RS-232C DB-9) ou Ethernet (RJ-45) para fins de gerenciamento via console;

2.3.38. Deve permitir o gerenciamento do equipamento através de interface WEB de forma nativa ao produto, através do protocolo seguro HTTPs;

2.3.39. Deve implementar classificação de tráfego nas camadas 2, 3 e 4;

2.3.40. Deve implementar Strict Priority;

2.3.41. Deve implementar WRR (Weighted Round Robin) ou SRR (Shaped Round Robin);

2.3.42. Deve suportar Inbound Rate Limiting;

2.3.43. Deve permitir a classificação, marcação e remarcação do

campo Type of Service (TOS) do cabeçalho IP;

2.3.44. O arquivo de configuração deve ser baseado em texto, permitindo seu Upload e Download;

2.3.45. Permitir, para implementar segurança, que apenas um MAC address fique configurado em uma porta e qualquer outro que tente se conectar a esta porta seja bloqueado;

2.3.46. Deve ser possível informar, por porta do switch, a quantidade de endereços MACs que podem ser aprendidos;

2.3.47. Deve suportar Broadcast Suppression, permitindo configurar valores individuais de supressão por porta;

2.3.48. Deve implementar no mínimo, 1005 VLANs ativas e permitir 4000 identificador de VLAN conforme o padrão IEEE 802.1Q;

2.3.49. Deve implementar funcionalidade para configurar portas protegidas e não protegidas dentro de uma VLAN, onde :

2.3.49.1. Portas protegidas não podem se comunicar com outras portas protegidas na mesma VLAN;

2.3.49.2. Portas não protegidas podem se comunicar com portas protegidas;

2.3.50. Deve implementar “MAC Authentication”;

2.3.51. Deve permitir a configuração de um texto “string” de identificação para cada porta do switch suportando no mínimo 30 caracteres;

2.3.52. Deve permitir uma temperatura de operação entre 0° até 45°C ou superior;

2.3.53. Deve possuir mecanismo que permita o acesso da estação de trabalho a rede através de uma VLAN default para os seguintes casos:

2.3.53.1. Quando a estação não possuir suporte ou configuração ativa para IEEE 802.1x; e

2.3.53.2. Quando ocorrer uma falha na autenticação IEEE 802.1x;

2.3.54. Deve implementar mecanismo de prevenção de "loops" nas portas frontais, permitindo o bloqueio da porta de forma automática, caso esta receba frames STP do tipo BPDU (Bridge Protocol Data Unit);

2.4. II.B – Switch de 48 portas, Quantidade _____

2.4.1. Deve ser montável em rack padrão EIA 19” (dezenove polegadas) e possuir kits completos para instalação;

2.4.2. Deve possuir, no mínimo, 48 (Quarenta e oito) portas 100/1000BaseTx em conectores do tipo RJ45 diretamente conectados ao equipamento, não sendo permitido o uso de conectores do tipo TELCO; Todas essas portas devem suportar o protocolo PoE (IEEE 802.3af);

2.4.3. Todas as 48 (quarenta e oito) portas devem suportar o protocolo PoE (IEEE 802.3af), disponibilizando 15 (quinze) watts de potência por porta;

2.4.4. 24 (vinte e quatro) portas devem suportar o protocolo PoE+ (IEEE 802.3at), disponibilizando 30 (trinta) watts de potência por porta;

2.4.5. Deve possuir, no mínimo, 2 (duas) portas 10/100/1000Base-X, tipo SFP MiniGbic, compatível com conectores ópticos do tipo LC, Multimodo, populadas com MiniGbics novos e originais;

2.4.6. Deve permitir o empilhamento através de interfaces específicas e fixas no equipamento para este fim, sem a necessidade de módulos adicionais, e com uma capacidade de largura de banda de no mínimo 32(trinta e dois) Gbps bidirecionais;

2.4.7. Deve possuir fonte de alimentação interna ao equipamento, que opere com tensões de entrada entre 100 e 240VAC e que suporte freqüência de 60 Hz nominais com tolerância de 5% para mais ou menos;

2.4.8. Deve suportar a instalação de fonte de energia redundante;

2.4.9. Deve permitir empilhar, no mínimo, 08 (oito) unidades e permitir o seu gerenciamento através de um único endereço IP;

2.4.10. Quando empilhado, deve permitir agregação de links (IEEE 802.3ad) entre quaisquer portas Gigabit, independentemente, das portas estarem em equipamentos diferentes da pilha;

2.4.11. Possuir capacidade de switching (Camada 2) de, no mínimo, 32 (trinta e dois) Gbps;

2.4.12. Possuir performance mínima a 48(quarenta e oito) Mpps;

2.4.13. Deve implementar funcionalidade de espelhamento de tráfego TX e RX, permitindo que as portas de origem e destino estejam em qualquer ponto da pilha;

2.4.14. Suportar, no mínimo, 8.000 (oito mil) endereços MAC;

2.4.15. Suportar gerenciamento via SNMP v1, v2c e v3;

2.4.16. Deve implementar IEEE 802.1p - (Classe de Serviços);

2.4.17. Deve implementar IEEE 802.1s - (Multiple Spanning Tree);

2.4.18. Deve implementar IEEE 802.1D - (Spanning Tree);

2.4.19. Deve implementar IEEE 802.1w – (Rapid Spanning Tree);

2.4.20. Deve implementar IEEE 802.3x – (Flow Control);

2.4.21. Deve implementar IEEE 802.1Q – (VLAN);

2.4.22. Deve implementar IEEE 802.3 ad (link aggregation), permitindo a criação de, no mínimo, 4 LAGs com 04 portas por LAG;

2.4.23. Deve implementar a RFC 3580 permitindo que um usuário autenticado por 802.1x seja automaticamente associado a sua respectiva VLAN;

2.4.24. Deve implementar IGMP v1, v2 e v3 e IGMP Snooping;

2.4.25. Deve implementar RADIUS client;

2.4.26. Deve ter suporte a Radius Authentication, Authorization e Accounting.

2.4.27. Deve implementar TFTP ou FTP client ;

2.4.28. Deve implementar Telnet;

2.4.29. Deve implemntar Syslog;

2.4.30. Deve implementar Command Line Interface – CLI;

2.4.31. Deve implementar Bridge MIB, RFC1493;

2.4.32. Deve implementar 4 (quatro) grupos RMON ;

2.4.33. Deve implementar MIB II, RFC1213;

2.4.34. Deve implementar RMON MIB, RFC 2819;

2.4.35. Deve implementar NTP ou SNTP;

2.4.36. Deve implementar Secured Shell (SSHv2);

2.4.37. Deve Possuir 1 (uma) porta RS-232C (DB-9) ou ethernet(RJ-45) para fins de gerenciamento via console;

2.4.38. Deve permitir o gerenciamento do equipamento através de interface WEB de forma nativa ao produto, através do protocolo seguro HTTPS;

2.4.39. Deve implementar classificação de tráfego nas camadas 2, 3 e 4;

2.4.40. Deve implementar Strict Priority;

2.4.41. Deve implementar WRR (Weighted Round Robin) ou SRR (Shaped Round Robin);

2.4.42. Deve suportar Inbound Rate Limiting;

2.4.43. Deve permitir a classificação, marcação e remarcação do campo Type of Service (TOS) do cabeçalho IP;

2.4.44. O arquivo de configuração deve ser baseado em texto, permitindo seu Upload e Download;

2.4.45. Permitir, para implementar segurança, que apenas um MAC address fique configurado em uma porta e qualquer outro que tente se conectar a esta porta seja bloqueado;

2.4.46. Deve ser possível informar, por porta do switch, a quantidade de endereços MACs que podem ser aprendidos;

2.4.47. Deve suportar Broadcast Suppression, permitindo configurar valores individuais de supressão por porta;

2.4.48. Deve implementar no mínimo, 1005 VLANs ativas e permitir 4000 identificador de VLAN conforme o padrão IEEE 802.1Q;

2.4.49. Deve implementar funcionalidade para configurar portas protegidas e não protegidas dentro de uma VLAN, onde :

2.4.49.1. Portas protegidas não podem se comunicar com outras portas protegidas na mesma VLAN;

2.4.49.2. Portas não protegidas podem se comunicar com portas protegidas;

2.4.50. Deve implementar “MAC Authentication”;

2.4.51. Deve permitir a configuração de um texto “string” de identificação para cada porta do switch suportando no mínimo 30 caracteres;

2.4.52. Deve permitir uma temperatura de operação entre 0° até 45°C ou superior;

2.4.53. Deve possuir mecanismo que permita o acesso da estação de trabalho a rede através de uma VLAN default para os seguintes casos:

2.4.53.1. Quando a estação não possuir suporte ou configuração ativa para 802.1x; e

2.4.53.2. Quando ocorrer uma falha na autenticação IEEE 802.1x;

2.4.53.3. Deve implementar mecanismo de prevenção de "loops" nas portas frontais, permitindo o bloqueio da porta de forma automática, caso esta receba frames STP do tipo BPDU (Bridge Protocol Data Unit);

ANEXO II

Equipamentos necessários para a prestação de serviços

A solução de controladora wireless deve ser capaz de gerenciar todos os access point descritos no item I.a e I.b do Termo de Referência.

A solução de gerenciamento deverá ser capaz de criar redes centralizadas, na quantidade de 20% dos APs adquiridos no TR ou em 1000 APs, o que for maior.

Caso os access points e o gerenciamento, descritos no item B, operem com todas as características técnicas do item A, utilizando processamento colaborativo e com gerencia centralizada, dispensa-se a necessidade do hardware da controladora.

Deve ser entregue rack de 19" e 44U para abrigar a solução de controladora e gerenciamento, com ventilação e espaçadores de patch cord inclusos.

O hardware do item A e item B de cada equipamento deverá obedecer ao tamanho de 19", do rack a ser entregue, e cada equipamento deverá possuir no máximo 4U, assim caso seja fornecido 2 (duas) controladoras e 2 (dois) gerenciamentos, não deverá superar a medida de 20U, contando com os espaçadores de patch cord.

Item A

1. **Requisitos Mínimos:**

   1.1. Hardware:

   1.1.1. Possuir, no mínimo, 02 (duas) interfaces Gigabit 1000Base-T e possibilitar ampliação para um total de, no mínimo 4 interfaces similares (inclusive as 02 já fornecidas).

   1.1.2. Possuir uma porta de serviço Ethernet 10/100/1000BaseT com conector RJ45.

   1.1.3. Deve Possuir 1 (uma) porta RS-232C (DB-9) ou Ethernet (RJ-45) para fins de gerenciamento via console.

   1.1.4. Possuir pelo menos uma fonte de alimentação elétrica interna.

   1.1.5. Possuir fonte redundante interna ao equipamento.

1.1.6. Possuir LEDS que indiquem: sistema ligado, interfaces de rede ativas, fonte de energia.

1.1.7. Deve ser instalável em Rack de 19”

1.2. Software:

1.2.1. Cada controladora deve ser capaz de gerenciar, no mínimo, 2000 (dois mil) Access-Points nos padrões IEEE 802.11b/g, 802.11a, 802.11n e 802.11ac simultaneamente.

1.2.2. O controlador WLAN deve ser capaz de controlar Access points nos padrões IEEE 802.11b/g, 802.11a e 802.11n simultaneamente.

1.2.3. Deverá implementar DHCP Server e Relay.

1.2.4. As licenças estão contempladas no fornecimento de cada access point.

1.2.5. Permitir uma topologia redundante N+1, provendo escalabilidade e alta disponibilidade. No caso de falha do Controlador WLAN, os access points relacionados deverão se associar à um controlador WLAN alternativo automaticamente.

1.2.6. Deve implementar servidor Syslog interno.

1.2.7. Permitir que APs registrados no controlador WLAN possam realizar o switching local (redes locais) do tráfego gerado entre os clientes a ele associados, sem a necessidade de utilização da rede WAN para o tráfego dos clientes de cada Access point.

1.2.8. Permitir que APs registrados no controlador WLAN possam realizar o switching central (redes centralizadas) do tráfego gerado entre os clientes a ele associados, utilizando a rede WAN para o tráfego dos clientes de cada Access point.

1.2.9. Em caso de falha do link WAN ou do próprio controlador, os clientes associados devem continuar tendo acesso à rede, inclusive, prover autenticação IEEE 802.1x para novos usuários.

1.2.10. Em caso de falha de um access point, o Controlador WLAN deve automaticamente ajustar a potencia dos access points adjacentes para dar cobertura de área onde o access point que falhou estava provendo o sinal. O aumento de potência não pode exceder os limites regulados pela ANATEL.

1.3. Segurança:

1.3.1. Implementar o padrão IEEE 802.11i com certificação WPA e WPA2.

1.3.2. Implementar WEP com chaves estáticas e dinâmicas (40 bits e 128 bits).

1.3.3. Implementar WPA com algoritmo de criptografia TKIP e Message Integrity Check.

1.3.4. Implementar WPA-2 (Wi-Fi Protected Access com algoritmo de criptografia AES).

1.3.5. Implementar IEEE 802.1X, com pelo menos os seguintes métodos EAP : EAP-MD5, EAP-FAST, PEAP-GTC, PEAP-MSCHAPv2 e EAP-TLS.

1.3.6. Deve ser capaz de autenticar usuários IEEE 802.1x utilizando o método PEAP sem a necessidade de servidor Radius Externo. Os usuários devem ser criados na base local do Controlador WLAN.

1.3.7. Implementar roaming(HAND-OVER) de um cliente autenticado entre os Access points.

1.3.8. Implementar mecanismo de autenticação através de portal Web para usuários visitantes.

1.3.9. Permitir a criação de um usuário especial para gerenciamento de usuários visitantes temporários.

1.3.10. Implementar mecanismo de autenticação, autorização e contabilidade (AAA).

1.3.11. Implementar o bloqueio da comunicação entre usuários em um mesmo SSID. Permitindo o isolamento dos usuários.

1.3.12. Implementar mecanismos para detecção, localização e contenção de Access points Rogue e clientes Rogue. O controlador WLAN deve gerar um alarme e localizar o Access point Rogue na planta baixa do local.

1.3.13. Implementar mecanismo para detecção, localização e contenção de Redes Ad-Hoc.

1.3.14. Implementar suporte a assinaturas de ataques de RF (rádio frequência) e prevenção de intrusão, auxiliando o administrador a customizar arquivos de assinatura de ataques, detectando rapidamente ataques de RF (rádio frequência) comuns tais como: denial of service (DoS), Netstumbler e FakeAP.

1.3.15. Implementar interface de gerenciamento de todas as funcionalidades localmente no controlador WLAN com suporte SSH , HTTPS via web browser, porta console e SNMP.

1.4. Gerência de Rádio Freqüência (RF)

1.4.1. Implementar ajuste dinâmico de canais 802.11 para otimizar a cobertura de rede e mudar as condições RF (rádio frequência) baseado em performance.

1.4.2. Implementar detecção de interferência e reajuste dos parâmetros de RF (rádio frequência) evitando problemas de cobertura e performance.

1.4.3. Implantar balanceamento de carga de usuários de modo automático através de múltiplos pontos de acesso, para otimizar o desempenho quando grande quantidade de usuários estão associados aos pontos de acesso.

1.4.4. Implementar mecanismos automáticos de gerenciamento de recursos de radio, detectando buracos de cobertura, indisponibilidades dos access points, executando auto-configuração, auto-correção e auto-otimizacão.

1.4.5. Implementar mecanismo que ajuste dinamicamente a saída de potência dos Access points individualmente para acomodar as condições de alterações da rede alterações, garantindo a performance e escalabilidade entre múltiplos access points para otimizar a performance durante elevada utilização da rede.

Item B

2. Solução de Gerenciamento:

2.1. A solução de Gerenciamento do Item I deverá ser capaz de gerenciar todos os Access points e controladoras descritas no item I do Termo de Referencia e item A deste anexo, se necessário.

2.2. Todo hardware e sistema operacional necessários para a instalação e operação da solução de gerenciamento, incluindo o servidor auxiliar de centralização de redes centralizadas, deverão ser fornecidos pela **CONTRATADA**, com redundância, e deverão ser capazes de cumprir os requisitos mínimos abaixo:

2.3. Este equipamento pode ser fornecido por qualquer fabricante;

2.4. Apenas o software deve ser do mesmo fabricante dos itens I do Termo de referencia e item A deste anexo;

2.5. REQUISITOS MÍNIMOS

2.5.1. A solução ofertada deverá ter capacidade de gerenciar simultaneamente, pelo menos, 10.000 (dez mil) access points.

2.5.2. A solução deverá ser entregue com capacidade inicial para gerenciar, no mínimo e simultaneamente, 500 (quinhentos) access points.

2.5.3. Deverá permitir o aumento gradativo da sua capacidade através de um módulo de expansão para solução de gerenciamento de rede wireless de forma a aumentar a capacidade de gerenciar e controlar os access points wireless até o limite da solução, sem gerar impacto no ambiente de produção.

2.5.4. Deve 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.

2.5.5. Deverá ser permitido o acesso ao software de gerência através de qualquer browser via HTTP ou HTTPS, permitindo o acesso à gerência de qualquer localidade que haja comunicação lógica com a plataforma.

2.5.6. Deve suportar a implantação de alta disponibilidade de modo redundante (ativo/standby).

2.5.7. Deve ter capacidade de permitir ao administrador do software a importar as plantas das localidades onde estão localizados os access points e assinalar as características de RF (rádio frequência) dos access points.

2.5.8. Deve permitir a organização hierárquica dos access points em plantas, de plantas em prédios e de prédios em projetos.

2.5.9. Todas as informações da rede devem ser apresentadas em uma console única e não devem ser separadas em consoles distintas, ou seja, deve haver gerência da rede que consolide a gerência dos elementos da rede.

2.5.10. Deve ter funcionalidade de descoberta automática dos dispositivos individuais da rede sem fio.

2.5.11. Deve permitir o aprovisionamento remoto dos elementos, inclusive alteração da configuração remota.

2.5.12. Deve permitir a visualização do mapa lógico da rede, com a representação dos equipamentos e sinalização de seu estado operacional por cores diferenciadas.

2.5.13. Deve permitir a visualização de alertas da rede em tempo real, com indicação de severidade por cores diferenciadas.

2.5.14. Deverá possuir ferramentas para permitir ao administrador visualizar, em um único console, o layout da rede sem fio e monitorar o desempenho desta rede, incluindo o mapa detalhado que exibe a cobertura de rádio freqüência sobre as plantas físicas das localidades atendidas.

2.5.15. Deve possibilitar a visualização de falhas na cobertura de rádio freqüência, alarmes e estatísticas de utilização, para fácil e rápido monitoramento e resolução de problema.

2.5.16. Deverá possuir ferramentas integradas para analisar os requerimentos de rádio freqüência para implantação da rede sem fio, incluindo a melhor localização para instalação dos access points na planta física da localidade, configuração e estimativa de desempenho e área de cobertura.

2.5.17. Deverá possuir meios de consolidação das informações da rede, tais como: interferência, níveis de ruído, relação sinal-ruído, potência de sinal e topologia de rede, permitindo ao administrador isolar e resolver problemas em vários níveis da rede sem fio.

2.5.18. Deverá ter capacidade de listagem on-line da relação sinal-ruído de cada usuário, sua localização, endereço IP, endereço MAC, nível de potência de recepção e dados de associação e de autenticação IEEE802.1x (quando utilizado).

2.5.19. Deve ter capacidade de identificar e listar os rádios vizinhos e respectivos SSID/BSSID que estão ao alcance de cada access point.

2.5.20. Deve ter capacidade de configurar alarmes automáticos, caso o índice relacionado ao alarme ultrapasse um determinado limite.

2.5.21. Deve gerar gráficos com análise de espectro “real-time”. Caso o software de gerenciamento não possua mecanismos para atender a este item, deverá ser fornecido software adicional para prover este serviço.

2.5.22. Deve ter capacidade de correlacionar alarmes de dois ou mais access points wireless para uma mesma fonte de interferência, e reportar ao administrador como um só dispositivo.

2.5.23. Deve permitir a configuração de, pelo menos, 8 (oito) grupos diferentes de usuários e administradores, com níveis de privilégios de acesso e configuração distintos.

2.5.24. Deverá permitir a criação de grupos para, pelo menos, agrupar os equipamentos. Deve possibilitar a associação de determinados usuários e administradores a estes grupos, de forma que apenas tenham acesso ao gerenciamento e visualização dos elementos pertencentes ao grupo em que foi associado.

2.5.25. Deverá ter capacidade de atualização do software/firmware dos access points de forma centralizada, via interface Web.

2.5.26. Deve ter capacidade de descobrir automaticamente os equipamentos individuais na infra-estrutura de rede wireless, eliminando a necessidade de configuração e manutenção locais e provendo informações para planejamento da capacidade e resolução de problemas.

2.5.27. Deverá suportar gerenciamento de falhas via SNMP (Simple Network Management Protocol) versão 3 (além do SNMP versão 2c e 1), para conexão segura entre a plataforma de gerência e os controladores wireless.

2.5.28. Deve ter capacidade de salvar modelos de configuração (templates), de forma a possibilitar a replicação desta configuração em outros equipamentos.

2.5.29. Deve ter capacidade de gerência da configuração, com armazenamento de diferentes versões de configuração e suporte para realizar "rollback”.

2.5.30. Deve ter capacidade de gerar alarmes quando detectado um ataque via rede sem fio.

2.5.31. Deve implementar a detecção, localização e contenção de Rogue APs e redes AD-HOC.

2.5.32. Deve implementar a detecção de clientes autorizados associados a access points não autorizados (Rogue APs), e de clientes não-autorizados em access points autorizados (clientes Rogue).

2.5.33. Deve implementar assinaturas de ataques de rádio freqüência e prevenção de intrusão para auxiliar o administrador a detectar rapidamente os ataques de RF (rádio frequência) do tipo “Denial of Service (DoS)”, “NetStumbler”, “Wellenreiter” e “Fake AP”.

2.5.34. Deve ser capaz de gerar relatórios personalizáveis para os administradores da rede.

2.5.35. Deve disponibilizar, no mínimo, os seguintes tipos de relatórios: listagem de clientes wireless, inventário da rede wireless, informações de configuração dos controladores wireless e dos access points, utilização da rede wireless e da rádio freqüência.

2.5.36. Deve disponibilizar relatórios para auditoria da rede (“Compliance Reports”). Deve ser gerado e disponibilizado, pelo menos, relatório no padrão “PCI Data Security Standard (DSS)” versão 1.1, apresentando informações de segurança da rede sem fio.

2.5.37. Deve disponibilizar relatórios das ameaças de segurança recorrentes antes que estas causem danos para a infra-estrutura das redes LAN e WLAN. Deve disponibilizar a geração de relatórios de segurança como, por exemplo, access points estranhos detectados na rede (Rogue AP e Adhoc Rogue).

2.5.38. Deve suportar a criação e aplicação de políticas que permitam o administrador gerenciar os seguintes itens:

2.5.38.1. VLAN;

2.5.38.2. Rádio Freqüência;

2.5.38.3. Qualidade de Serviço (QoS);

2.5.38.4. Políticas de segurança;

2.5.38.5. SSIDs múltiplos e únicos com parâmetros individuais de segurança.

2.5.39. Deve implementar ferramentas de resolução de problemas de clientes com dificuldades para se associarem à rede wireless.

2.5.40. Sistema de gerenciamento deverá ser fornecido em “appliance” ou em servidor específico para a função de gerenciamento.

2.5.41. “appliance” ou servidor disponibilizado para o sistema de gerenciamento deverá ser fornecido de forma a suportar a capacidade máxima do sistema de gerenciamento ofertado, sem apresentar falhas e/ou excesso de consumo de CPU, memória e discos rígido, com limite máximo de utilização de 75% (setenta e cinco por cento) do hardware.

2.5.42. Equipamento ofertado deverá ter, no máximo, 2 RU (dois “rack unit”) de altura e deverá ser instalável em rack padrão de 19 (dezenove) polegadas, sendo fornecido com todos os acessórios necessários para sua montagem.

2.5.43. Deverá possuir, no mínimo, 2 (duas) fontes de alimentação de energia, para efeito de redundância, com seleção automática de tensão (100-240 VAC) 60Hz.

2.5.44. Deverá ser fornecido com todos os itens necessários para operacionalização do equipamento, tais como: softwares, licenças, cabos de console, cabos de energia elétrica, documentações técnicas e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento.

2.5.45. Caso os access points e o gerenciamento, descritos no item B, operem com todas as características de controladora, utilizando processamento colaborativo e com gerencia centralizada, é necessário que este servidor, ou outro auxiliar, de gerenciamento faça a função de centralizador de redes centralizadas.