ANEXO IV

Referente ao Edital de Pregão nº. 016/2015

Especificações Técnicas

1. OBJETIVO

Implantação de rede Wi-Fi na sede da DMED situada na Rua Amazonas, 65 – Centro – Poços de Caldas – MG – 37701-008. Junto à rede Wi-FI deverão ser entregues plataforma de gerenciamento, plataforma de controle de acesso e treinamentos conforme especificações.

OBSERVAÇÃO: As certificações exigidas no corpo dessa especificação técnica serão exigidas no momento da apresentação da proposta.

2. DESCRIÇÃO DO EQUIPAMENTO

GRUPO	ITEM	DESCRIÇÃO DO EQUIPAMENTO	QUANTIDADE
1	1	Controlador Wireless	1
	2	Conjunto de Pontos de Acesso	1
	3	Plataforma de Gerência e Controle de Acesso	1
	4	Treinamento Tipo 1	1
	5	Treinamento Tipo 2	1
	6	Instalação Física	1

A DMED concederá visita técnica ao local de instalação e, em seguida, uma reunião técnica será realizada para elucidar possíveis dúvidas.

O evento deverá ser agendado previamente com o Sr. Anderson Stano Durelli pelo e-mail adurelli@dmedsa.com.br indicando o número de participantes para o provisionamento necessário. A data limite para realização da visita técnica será de 02 (dois) dias úteis anteriores a data marcada para a abertura da licitação.

It.1: Controlador Wireless [Quantidade: 1 unidade]

2.1.1. Características Básicas

- O controlador wireless deverá ser fornecido em forma de appliance virtual para plataforma VMWare.

2.2.1. Capacidade de Controle de Ponto de acessos

- Gerenciar, no mínimo, 24 (vinte e quatro) Ponto de acessos (APs) simultaneamente.

- Suportar a expansão do número de ponto de acessos através de licenças adicionais, sem exigir a troca de hardware ou host VMWare.
- Suportar a expansão de capacidade através de licenças de software para, no mínimo, 250 (duzentos e cinquenta) APs por controlador.
- Suportar o gerenciamento simultâneo de, no mínimo, 4.096 (quatro mil e noventa e seis) usuários por controlador.

2.3.1. Modo de Operação

- O controlador WLAN poderá estar instalado em qualquer ponto da infraestrutura de rede e deve possuir a capacidade de controlar APs instalados na mesma localidade e/ou em localidade remota através de rede WAN;
- Na ocorrência de inoperância de um AP, o controlador WLAN deverá ajustar automaticamente a potência dos APs adjacentes, de modo a prover a cobertura da área não assistida;
- O controlador deve permitir configuração em alta disponibilidade (HA) com outro controlador de igual capacidade;
    - Se controlador principal falhar, os APs relacionados no controlador principal devem ser gerenciados pelo controlador redundante sem a necessidade de intervenção ou reconfiguração;
    - Quando um dos controladores de um par configurado como HA falhar, o controlador que restar deverá ter capacidade de assumir todos os APs e usuários do controlador com falha, adicionalmente aos APs adotados por ele e não permitindo que a rede wireless se torne inoperante;
    - **NÃO** deverá ser fornecido com a solução controlador adicional nem licença para HA. Somente deverá ser provido suporte para essa configuração;
- Implantar sistema de balanceamento de carga para associação de clientes entre APs próximos, para otimizar a performance;
- Detectar áreas de sombra de cobertura e efetuar os devidos ajustes para sua correção automaticamente;
- Ajustar dinamicamente o nível de potência e canal de rádio dos APs, de modo a otimizar o tamanho da célula de RF, garantindo a performance e escalabilidade;
- Implantar Dynamic Radio Management (DRM) ou função semelhante de controle de rádio frequência (Canal e potência);
- Implantar modo de operação com encaminhamento de tráfego diretamente no Ponto de acesso (AP), ou seja, switching no AP;
- Implantar modo de operação tunelado do tráfego wireless diretamente no controlador wireless;

- Deve ser possível usar os dois modos (Switching no AP e tráfego tunelado) simultaneamente;

2.4.1. Roteamento

- Deve possibilitar a configuração de rotas estáticas e via protocolo OSPF.
- Deve possuir DHCP relay.

2.5.1. Gerenciamento

- Implantar:
  - RFC 3164 Syslog;
  - SSH v2 Secure Shell v2;
  - Telnet;
  - TFTP;
  - CLI (Command Line Interface);
- Permitir a atualização remota do sistema operacional e dos arquivos de configuração utilizados no equipamento;
- Permitir a configuração e gerenciamento seguro por meio de browser padrão (HTTPS);
- Possuir ferramentas de debug e log de eventos para depuração e gerenciamento em primeiro nível;

2.6.1. Funcionalidades Gerais

- Implementar em conjunto com os Ponto de acessos os padrões: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, 802.1d.
- Implementar as seguintes RFCs: RFC 2865 Radius, RFC 2866 Radius Accounting, RFC 2165, 2608 SLP, RFC 2131 DHCP, RFC 2328 OSPF, RFC 1350 TFTP Protocol, RFC 1155 MIB-I, RFC 1213 MIB-II, RFC 3576 Dynamic Authentication Extensions, RFC 1305 NTP.
- Deve implementar mecanismo do tipo RF Auto-Tuning, ou seja, associar dinamicamente o canal de comunicação e a potência de transmissão dos rádios dos pontos de acesso e ainda reajustar estes parâmetros de forma automática sempre que for necessário.
- Deve implementar servidor DHCP.
- Implantar, em conjunto com o Ponto de Acesso, Qualidade de Serviço com suporte a IEEE 802.11e e WMM.
- Implantar suporte a CAC (CallAdmissionControl).
- Possibilitar roaming com integridade de sessão, dando suporte a aplicações em tempo real, tais como, VoWLAN e streaming de vídeo.
- Implantar suporte a economia de energia com o uso do UAPSD (Unscheduled Automatic Power Save Delivery).
- Implantar, em conjunto com o AP, o fast roaming seguro.
- Implantar 802.1Q.

- Implantar padrão 802.1p.
- Implantar mapeamento de QoS de pacotes marcados na rede cabeada com TOS/DSCP para a rede wireless através de WMM.
- Implantar protocolo de autenticação para controle do acesso administrativo ao equipamento utilizando servidor RADIUS ou TACACS+.
- Suportar a autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário.
- Implantar listas de controle de acesso ou funcionalidade similar de controle.
- Implantar filtros de acesso à rede baseados em endereços MAC.
- Implantar associação dinâmica de usuário a VLAN, com base nos parâmetros da etapa de autenticação.
- Implantar associação dinâmica de filtros ou ACL e de QoS, com base nos parâmetros da etapa de autenticação.
- Implantar IEEE 802.11i.
- Implantar IEEE 802.1X, para autenticação de clientes wireless, com pelo menos os seguintes métodos EAP: EAP-TTLS, PEAP e EAP-TLS.
- Implantar a integração com RADIUS Server que suporte os métodos EAP citados.
- Implantar a limitação de banda por usuário ou grupo.
- Implantar, em conjunto com o AP, WEP, chaves estáticas e dinâmicas.
- Implantar, em conjunto com o AP, WPA com algoritmo de criptografia TKIP.
- Implantar, em conjunto com o AP, WPA2 com algoritmo de criptografia AES.
- Deve possuir localmente no controlador, portal web para autenticação dos usuários visitantes, sendo possível a customização com informações e características visuais (mensagem, logo, banner, etc).
- Deverá disponibilizar usuário específico para a administração e gerência do portal web, sendo que este usuário não deve ter acesso as outras informações e configurações do controlador.
- O portal web de autenticação, bem como a ferramenta de administração e gerência devem ser acessadas via web nativo, sem a necessidade de instalação de nenhum software ou plug-in adicional.
- A base de usuários visitantes deve ser interna ao controlador, não sendo necessário alterações (inclusão/exclusão/alteração) na base de dados dos usuários Active Directory/LDAP.
- A ferramenta de criação dos usuários visitantes deverá ter uma página onde constem as informações de conta e políticas de uso da instituição, sendo possível a impressão destas informações para entrega ao visitante no momento do registro.

- A criação das contas de visitantes deve possibilitar a criação de no mínimo os seguintes parâmetros:
  - Nome do usuário;
  - Senha;
  - Data de início e término de validade;
  - Tempo de sessão;
  - Horário permitido;
- Deve permitir o uso de captive portal externo ao controlador. Caso sejam necessárias licenças ou hardware específico os mesmos devem ser fornecidos.
- Deve permitir autenticação utilizando base de usuários disponibilizados pelo dispositivo de controle de acesso ofertado como parte da solução.

2.7.1. Garantia

- O **Controlador Wireless** deve permitir atualizações e suporte técnico pelo período de 36 (trinta e seis) meses.
- O Fabricante deverá disponibilizar gratuitamente, durante o período de garantia, suporte e atualização dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança.
- Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais.
- Os chamados técnicos deverão ser gerenciados pela LICITANTE em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos.

2.8.1. Compatibilidade

- Os componentes do **Controlador Wireless** deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento.
- O **Controlador Wireless** especificado neste item deve ser totalmente compatível e do mesmo fabricante do Ponto de Acesso (item 2).
- O **Controlador Wireless** especificado neste item deve ser totalmente compatível e do mesmo fabricante da Plataforma de Gerência e Controle de Acesso (item 3).

It.2: Ponto de Acesso [Quantidade: 18 unidades]

- **Características Básicas**
  - Ponto de Acesso deve atender simultaneamente aos padrões: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac.

- Permitir a conexão simultânea de dispositivos configurados nos padrões: IEEE 802.11b/g/n, IEEE 802.11a/n, IEEE 802.11ac.
- Implantar funcionamento simultâneo dos rádios 2.4Ghz e 5.0 Ghz
- Implantar todas as seguintes taxas de transmissão e fallback automático:
- IEEE 802.11a: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps;
    - IEEE 802.11b: 11, 5.5, 2 e 1 Mbps
    - IEEE 802.11g: 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2 e 1 Mbps;
    - IEEE 802.11n: 300, 270, 180, 120, 60, 45, 30 e 15 Mbps;
    - IEEE 802.11n: 450, 300, 270, 180, 120, 60, 45, 30 e 15 Mbps;
    - IEEE 802.11ac: 866.7, 780, 390, 260, 130, 97.5, 65 e 32.5 Mbps;
- Possuir e acompanhar componentes que permita sua fixação em teto e parede;
- Ponto de Acesso deve ser eficientemente energizados e usar até 9.6 Watts com todas as funcionalidades habilitadas.
- Ponto de Acesso deve suportar performance em conexão cabeada de 40.000pps.
- Ponto de Acesso deve implementar instalação plug and play.
- Ponto de Acesso devem implementar análise de espectro RF
- Ponto de Acesso devem implementar um modo hibrido de operação que seja capaz de suportar varredura de segurança e atender os clientes no mesmo rádio.
- Transmissão máxima de potência de cada rádio deve ser de pelo menos 26dBm para 5GHz e 25dBm para 2.4GHz.

- **Portas de Rede**
    - Possuir pelo menos 1 (uma) porta Gigabit Ethernet 10/100/1000 Mbps, auto-sensing, com conector RJ-45 Fêmea para dados, não sendo aceito portas de gerência;
    - Suportar energização, pela interface de rede, através de um único injetor padrão IEEE 802.3af PoE;
    - O AP deve permitir sua operação em capacidade máxima mesmo quando energizado através do injetor PoE;
    - O AP deve suportar sua energização através de fonte externa ou interna que opere com tensão de entrada para a fonte, em 110-200Vac;
- **LED's e Sinalização**
    - Possuir LEDs indicativos do estado de operação.
    - Possuir LEDs indicativos da atividade dos rádios.
- **Antenas.**
    - Possuir antenas internas ao Ponto de acesso, em conformidade com o padrão IEEE 802.11a/b/g/n/ac.
    - Possuir ganho de, pelo menos, 3 dBi para 2.4GHz.

- Possuir ganho de, pelo menos, 5dBi para 5.0GHz.
- Implantar padrão de irradiação omnidirecional.
- Implantar operação simultânea em 2x2:2 MIMO.

- **Modo de Operação**
  - Implantar modo de operação onde o AP possa estar remotamente conectado ao controlador wireless tanto de forma direta em uma rede de camada 2 ou em qualquer ponto de uma rede segmentada em subredes de camada 3;
  - O ponto de acesso deve permitir sua operação através da conexão a um controlador principal e a um controlador secundário;
  - Selecionar automaticamente o canal de transmissão;
  - Ajustar dinamicamente o nível de potência e canal de rádio;
  - Possuir suporte a pelo menos 8 SSIDs para 2.4Ghz e 8 SSIDs para 5.0Ghz;
  - Permitir habilitar e desabilitar a divulgação do SSID;
  - Deve implementar Fast Roaming ou funcionalidade similar de forma a garantir o Roaming sem perda de conexão;
  - Não deve haver licença restringindo o número de usuários por AP.
  - Implantar a pilha de protocolos TCP/IP;
  - Implantar VLANs conforme padrão IEEE 802.1Q;
  - Implantar cliente DHCP, para configuração automática de rede;
  - Configurar-se automaticamente ao ser conectado na rede;
  - Implementar Packet aggregation A-MPDU, A-MSDU para 802.11ac e 802.11n.
- **Gerenciamento**
  - Permitir via controlador wireless, a atualização remota do sistema operacional.
  - Permitir via controlador wireless, a atualização remota dos arquivos de configuração utilizados no equipamento.
  - Implantar funcionamento em modo gerenciado pelo controlador wireless.
- **Segurança e QoS**
  - Possuir entrada para dispositivo antifurto do tipo Kensingtonlock ou similar;
  - Suportar varredura de Rádio Frequência nas tecnologias 802.11a, 802.11b/g, 802.11n e 802.11ac para identificação de AP não autorizados (rogues);
  - Suportar varredura de Rádio Frequência nas tecnologias 802.11a, 802.11b/g, 802.11n, 802.11ac para identificação de interferências nos canais na rede WLAN;
  - Implementar IEEE 802.1x de acesso do próprio AP a rede cabeada;
  - Implementar autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário;
  - Implementar em conjunto com o Controlador WLAN, WEP, chaves estáticas e dinâmicas;

- Implementar em conjunto com o Controlador WLAN, WPA com algoritmo de criptografia TKIP e MIC;
- Implementar em conjunto com o Controlador WLAN, WPA2 com algoritmo de criptografia AES;
- Implementar padrão IEEE 802.11e WMM para priorização de tráfego, suportando aplicações em tempo real, tais como VoIP e vídeo;
- Deve implementar um modo de operação que seja capaz de fazer a varredura de segurança, trabalhando de forma dedicada, sem a necessidade de módulos de hardware adicionais para este fim.
- O AP deve suportar, em modo de operação WIPS dedicado, sua conexão a um controlador principal ou controlador secundário, realizando detecção de: Rogue AP, Honeypot, Packet Injection, Redes Ad Hoc, Main-in-the-middle, Negação de Serviço (DoS), MAC Spoofing, Tentativa de quebra de chaves, Reconhecimento de rede.

- **Certificações**
  - Possuir certificação/homologação da ANATEL.
- **Garantia**
  - O Ponto de Acesso deverá possuir garantia do fabricante LIFETIME, sendo limitada a 60 (sessenta) meses após a descontinuação (End-of-Sale) do equipamento.
  - Nos casos de troca de equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais.
  - O Fabricante deverá disponibilizar gratuitamente suporte e atualização dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança.
  - Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais.
  - Os chamados técnicos deverão ser gerenciados pela LICITANTE em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos.
- **Compatibilidade**
  - Os componentes do Ponto de Acesso deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento.
  - Todos os componentes do Ponto de Acesso deverão ser compatíveis entre si, com o conjunto do equipamento e com suas funcionalidades, sem a utilização de adaptadores, fresagens, pinturas, usinagens em geral, furações, emprego

de adesivos, fitas adesivas ou quaisquer outros procedimentos ou emprego de materiais inadequados ou que visem adaptar forçadamente o equipamento ou suas partes que sejam fisicamente ou logicamente incompatíveis. (Será aceito o regime de OEM desde que comprovado pelo próprio fabricante).

- O Ponto de Acesso especificado neste item deve ser, obrigatoriamente, do mesmo fabricante e ser gerenciado via controlador wireless (item 1).
- O Ponto de Acesso especificado neste item deve ser totalmente compatível e do mesmo fabricante da Plataforma de Gerência e Controle de Acesso (item 3).

It.3: Plataforma de Gerência e Controle de Acesso [Quantidade: 1 unidade]

1. Características Básicas

- Todas as licenças necessárias para o funcionamento da solução devem ser fornecidas, incluindo sistema operacional, banco de dados, etc.
- O software deverá contemplar em uma mesma licença, plataforma de gerência e controle de acesso descritos nesta especificação.

2. Funcionalidades Gerais: Plataforma de Gerência

- Deve permitir que, no mínimo, 25 usuários administrativos acessem a ferramenta de gerenciamento simultaneamente.
- A plataforma deve ser licenciada para gerência de, no mínimo, 50 (cinquenta) dispositivos IP do ambiente de rede.
- Cada pilha de switches deve ser contabilizada como 1 (um) endereço IP, independentemente da quantidade de unidades na pilha.
- A plataforma deve ter capacidade de gerenciar, no mínimo, 500 (quinhentos) Pontos de acesso (APs).
- A plataforma deve possuir arquitetura cliente servidor, com interface WEB ou java podendo ser acessível através de browser WEB padrão.
- A plataforma deve possibilitar a configuração de diferentes perfis de administradores. Deve ser possível ainda criar usuários com perfil de administração e outros de apenas visualização.
- A plataforma deve permitir o gerenciamento de configurações, desempenho e falhas na rede.
- A plataforma deve permitir sua instalação em pelo menos uma das plataformas abaixo:
  - Windows em versões 32 ou 64 bits.
  - LINUX: Red Hat Enterprise Linux versão 5 ou mais recente e nas plataformas de 32 ou 64 bits.
  - Appliance virtual Vmware ESXi 4 64 bits ou superior.

- A plataforma de gerenciamento deve suportar o protocolo SNMP de gerenciamento de versão 1, 2 e 3.
- A plataforma de gerenciamento fornecida deve ser capaz de gerenciar equipamentos de outros fabricantes, pelo menos de forma básica.
- A plataforma de gerenciamento deve permitir o descobrimento de equipamentos presentes em uma ou mais sub-redes, a fim de garantir uma auditoria constante na infraestrutura de TI.
- A plataforma de gerenciamento deve permitir a criação de topologias/mapas da infraestrutura de rede através de protocolos de descobrimento.
- O mapa deve permitir a identificação de problemas na infraestrutura de rede através de mudança de cores.
- Permitir a visão agrupada da topologia conforme configuração do usuário.
- A plataforma de gerenciamento deve permitir a criação, edição, remoção de VLANs nos dispositivo e associação das portas as mesmas.
- A plataforma de gerenciamento deve permitir a identificação do status das portas dos dispositivos up ou down, tecnologia e velocidade das portas.
- A plataforma de gerenciamento deve permitir a configuração de alarmes quando algum trap/evento ocorrer na rede.
- A plataforma deve permitir a configuração gráfica de um servidor SMTP externo para o envio de informações de gerenciamento da plataforma.
- A plataforma de gerenciamento deve permitir envio de e-mail ou execução de um script ou programa integrado com a plataforma para alertas.
- A plataforma deve permitir o gerenciamento dos dispositivos através de uma página WEB.
- A plataforma de gerenciamento deve permitir a localização de um dispositivo da rede baseado nos argumentos endereço IP, endereço MAC, user name e sub-rede.
- A solução deverá prover recursos de "troubleshooting" capaz de mostrar por meio do RMON, dados presentes nos switches como performance ou estatísticas de utilização.
- A plataforma de gerenciamento deve permitir o gerenciamento das configurações de filas e priorização de tráfego dos dispositivos da rede.
- A plataforma de gerenciamento deve permitir a criação de perfis de classificação do tráfego nos dispositivos, baseado em usuários.
- A plataforma de gerenciamento deve permitir a criação e o gerenciamento de políticas de acesso a rede nos dispositivos.
- A plataforma de gerenciamento deve suportar e gerenciar graficamente as características de autenticação padrão IEEE 802.1X e via MAC.

- A plataforma de gerenciamento deve permitir a configuração para atribuição de perfil de usuário com regras e QoS especifico conforme autenticação do usuário.
- A plataforma de gerenciamento deve permitir a configuração gráfica de rate limit nos equipamentos gerenciados.
- A plataforma de gerenciamento deve permitir a configuração estática e dinâmica da funcionalidade MAC Locking ou Port Security, para executar o LOCK de MAC Address na rede.
- A plataforma de gerenciamento deve permitir a configuração gráfica de vários métodos de autenticação, atendendo, no mínimo, a configuração da autenticação WEB, autenticação MAC, autenticação IEEE 802.1X.
- A plataforma deve permitir o inventário detalhado de atributos dos dispositivos da rede, atendendo, no mínimo, números seriais, versão do sistema operacional e memória.
- A plataforma de gerenciamento deve permitir o armazenamento das configurações dos dispositivos.
- A plataforma de gerenciamento deve permitir o agendamento da função de armazenamento de configuração de determinados elementos da rede. O agendamento deve ter periodicidade mínima de um dia.
- A plataforma deve permitir a comparação da configuração atual do dispositivo com a configuração armazenada na plataforma.
- Deve permitir o upgrade do sistema operacional ou Boot Prom dos dispositivos, unitariamente e para um grupo de dispositivos, inclusive podendo agendar um dia e horário para que este upgrade aconteça automaticamente.
- A plataforma deve permitir a execução do reset dos dispositivos.
- A plataforma deve pemitir restaurar a configuração armazenada. Deve ser possível ainda aplicar essa configuração em um equipamento em processo de substituição.
- A plataforma deve ser capaz de coletar e exibir informações de Netflow recebidas dos equipamentos de rede.
- A plataforma deve ser acessível através de dispositivos móveis tais como iPad, iPhone e Android.
- A plataforma deve possuir capacidade de importar mapas ou plantas de cada localidade.
- A plataforma deve permitir a visualização da localização de determinado usuário em um mapa carregado na plataforma.
- A plataforma deve ser capaz de controlar e gerenciar todas as funcionalidades presentes nos Controladores Wireless, Sensores WIPS e Ponto de acessos em uma mesma console de gerenciamento.

- O software de gerenciamento deve implantar a gerência de configuração através de interface gráfica dos controladores wireless, sensores WIPS e ponto de acessos.
- O software de gerenciamento deve permitir a configuração de parâmetros de QoS nos controladores wireless e ponto de acessos.
- O software de gerenciamento deve permitir a configuração de regras de controle de acesso nos controladores wireless e ponto de acessos.
- Deve implementar a gerência de configuração centralizada de soluções wireless.
- Deve suportar a cobertura de rádio frequência de cada AP, facilitando a localização de problemas.
- Deve possibilitar a visualização de informações de clientes incluindo: Endereço MAC, potência do sinal, taxa de transmissão, SSID, canais utilizados e AP e controladores aos quais está associado.
- A plataforma deverá prover relatórios sobre os sensores que trabalham de forma dedicada (“full-time”) monitorando o ambiente de RF de forma continua.
- A plataforma deverá prover relatórios sobre os sensores que trabalham de forma parcial monitorando o ambiente de RF de forma continua.
- A plataforma deve prover relatórios contendo a autoclassificação de clientes e equipamentos externos ao ambiente da contratante permitindo uma coexistência no ambiente de RF.
- Deve apresentar relatórios com as seguintes categorias de ameaças de um ambiente wireless: Rogue AP, Redes Ad hoc, Injeção de Pacotes, Negação de Serviço (DoS), MAC Spoofing, man-in the-midlle, Quebra de chave.
- Localizar e rastrear clientes, dispositivos móveis e Aps na planta;
- Ilustrar na planta da contratante a visualização de cobertura do ambiente de RF, bem como, distribuição de canais em 2.4 GHz e 5.0GHz;
- Permitir captura de pacotes no ambiente WiFi e integrar com analisador de pacotes Wireshark.
- Alertar sobre problemas de interferência de RF ou intermitência de conectividade existente no ambiente.
- A plataforma de gerência deve ser capaz de fornecer relatórios históricos de tráfego de wireless.
- A plataforma de gerência deve fornecer dashboards da rede cabeada e sem fio, com capacidades de detalhamento.
- A plataforma de gerência deve fornecer detalhes de identidade e informações de acesso.
- A plataforma de gerência deve fornecer relatórios customizados para histórico e dados em tempo real.

- A plataforma de gerência deve fornecer visualização e busca de clientes e seus dispositivos móveis.
- A plataforma de gerência deve fornecer uma visibilidade abrangente de todos os dispositivos móveis na infraestrutura.
- Deve fornecer XML APIs abertas para integração com aplicações de terceiros.

3. Funcionalidades Gerais: Controle de Acesso

- Deve permitir a verificação e uso em no mínimo 500 (quinhentos) dispositivos/usuários.
- Implementar controle de acesso à rede através de autenticação e da verificação de requisitos pré-estabelecidos, de forma a permitir, ou não, a conexão de dispositivos/usuários à rede.
- O processo de autenticação deverá seguir o padrão IEEE 802.1X ou método similar que utilize protocolo seguro SSL em conjunto com servidor de políticas, e deverá permitir a alteração da VLAN do usuário conforme o perfil do mesmo.
- Deverá permitir autenticação via LDAP.
- Permitir a verificação dos seguintes itens nas estações de trabalho com sistema operacional Windows:
  - Versão do Windows e Service Pack;
  - Chaves do Registro do Windows;
  - Pacotes de atualização do Windows aplicados;
  - Existência de software antivírus instalado;
  - Status do software antivírus (habilitado ou desabilitado);
  - Se a versão e as bases de assinaturas do antivírus estão atualizadas;
- Suportar a configuração de diversas funções, incluindo visitantes e convidados, e permitir políticas de admissão diferentes para cada função.
- Suportar o controle de acesso para redes cabeadas e sem fio.
- Possibilitar o acesso a convidados através de autorização explícita do funcionário responsável pelo convidado.
- Permitir a criação de políticas customizáveis conforme o sistema operacional da estação sendo validada ou conforme o domínio de segurança configurado.
- Permitir a segregação de funções administrativas, conforme perfil de acesso (administrador de rede, administrador de segurança, help desk, etc). Essa função pode ser realizada via Ferramenta de Administração.
- Permitir o backup e a restauração das políticas e configurações, diretamente no equipamento da solução ou via Ferramenta de Administração.
- Suportar o envio de alarmes para um servidor SYSLOG externo.
- Capacidade de visualização das seguintes informações:
  - Nome do Usuário;
  - Endereço MAC do usuário;

- Endereço IP do usuário;
- Perfil do usuário;
- Sistema Operacional do usuário;
- Resultado do processo de controle de acesso à rede.

- A Plataforma de Controle de Acesso deverá apresentar informações de conexão de todos os dispositivos conectados diretamente a plataforma. Deverá ser possível visualizar, no mínimo, as seguintes informações:
  - Endereço MAC e IP;
  - Endereço do switch o qual o dispositivo está conectado;
  - Porta do switch o qual o dispositivo está conectado;
  - Estado do dispositivo: aceito, em quarentena, rejeitado e desconectado;
  - Nome de Usuário;
  - Sistema Operacional do usuário;
  - Host;
  - Tipo do dispositivo: celular, PC, tablet etc;
  - Fabricante do dispositivo;
  - Tipo de autenticação;
  - Perfil ao qual o dispositivo foi direcionado;
- A Plataforma de controle de acesso deverá permitir atribuir perfis baseado no tipo de dispositivo conectado (celular, PC, tablete, etc).

4. Garantia

- A Plataforma de Gerência e Controle de Acesso deve permitir atualizações e suporte técnico pelo período de 36 (trinta e seis) meses.
- O Fabricante deverá disponibilizar gratuitamente, durante o período de garantia, suporte e atualização dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança.
- Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais.
- Os chamados técnicos deverão ser gerenciados pela LICITANTE em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos.

5. Compatibilidade

- A Plataforma de Gerência e Controle de Acesso especificada neste item, deve ser totalmente compatível com os switches Extreme Networks Summit X440, X450 e X670, já adquiridos e em operação na DME Distribuição S/A - DMED.

- A Plataforma de Gerência e Controle de Acesso especificada neste item, deve ser do mesmo fabricante e totalmente compatível, incluindo todas as funcionalidades citadas, com o Controlador Wireless (item 1) e Ponto de Acesso (item 2).

It.4: Treinamento Tipo 1 [Quantidade: 1 unidade]

1. Características Gerais

- Capacitar os participantes a realizar atividades de configuração e gestão de uma rede Wireless, se utilizando de softwares de gerenciamento de rede. Este conhecimento deve ser reforçado através de atividades práticas com equipamentos de rede em um ambiente de laboratório, onde os alunos deverão executar atividades reais de configuração de pontos de acesso, parâmetros de segurança, filtros e configuração de privacidade e gestão.
- Após a conclusão deste treinamento, os alunos deverão ter adquirido conhecimento suficiente para se configurar, gerenciar e implantar um ambiente de rede Wireless.
- O treinamento deve ter carga horária de 32 (trinta e duas) horas.
- Ao final do treinamento, deverá ser entregue certificado de participação no treinamento a todos os participantes.
- Deverá ser realizado nas dependências do Fabricante, com ambiente de laboratório funcional.
- Deverá ser fornecido em unidades de 1 (uma) semana, para 2 (dois) participantes indicados pela Contratante.

2. Conteúdo / Agenda

- Visão geral dos componentes e arquitetura de um ambiente de rede Wireless.
- Configuração de controladores wireless, pontos de acesso e rede virtual.
- Configuração e implementação de parâmetros de segurança, incluindo, 802.1x, filtros (políticas), privacidade e captive portal.
- Introdução a gestão de uma WLAN incluindo a configuração de parâmetros de qualidade de serviço (QoS), classe de serviço (CoS) e configurações de gerenciamento de usuário.
- Visão geral sobre alta capacidade, mobilidade, solução de problemas e manutenção geral do controlador wireless.
- Discussões sobre a funcionalidade de segurança IDS/IPS no controlador wireless, a fim de detectar e mitigar ameaças de segurança de forma proativa.
- Visão geral de wireless logs e reports.

It.5: Treinamento Tipo 2 [Quantidade: 1 unidade]

1. Características Gerais

- Deve ser apresentado aos funcionários participantes a plataforma de gerência responsável por controlar e gerenciar todas as funcionalidades dos equipamentos descritos em uma mesma suíte (mesma console de gerenciamento). Se utilizando de Open Systems Interconnection (OSI) e Network Management Model (NMM), o conhecimento deve ser reforçado através de atividades práticas em uma rede pré-configurada. Estas atividades devem ser reais, como por exemplo, configuração, performance, falhas, segurança etc.
- Após a conclusão deste treinamento, os alunos deverão ter adquirido conhecimento suficiente para se configurar e gerenciar redes wired e wireless se utilizando da plataforma de gerência e controle de acesso ofertada.
- O treinamento deve ter carga horária de 32 (trinta e duas) horas.
- Ao final do treinamento, deverá ser entregue certificado de participação no treinamento a todos os participantes.
- Deverá ser realizado nas dependências do Fabricante, com ambiente de laboratório funcional.
- Deverá ser fornecido em unidades de 1 (uma) semana, para 2 (dois) participantes indicados pela Contratante.

2. Conteúdo / Agenda

- Discussões de como se identificar cada dispositivo, conexões, componentes, software, imagem e versão do bootrom. Em adicional também deverá existir atividades de como se coletar configurações, rastrear alterações na configuração e restaurar caso necessário.
- Discussão em torno de gerenciamento de falha usando de configuração de alarmes para se detectar, identificar e registrar falhas no log e notificar os usuários sobre problemas na rede a fim de evitar paralisações desnecessárias ou perda de dados.
- Discussões em torno de gestão de desempenho a fim de se identificar e monitorar taxas de transferência, utilização e taxas de erro. As atividades também deverão ter foco no uso de Qualidade de Serviço (QoS) e classe de serviço (CoS), como forma de se controlar o tráfego.
- Visão geral sobre gestão de segurança destacando quais ferramentas devem ser utilizadas a fim de se controlar o acesso à rede e para se proteger dados.

It.6: Instalação Física [Quantidade: 1 unidade]

1. Características Gerais

- A contratada deverá fornecer todo material necessário para a instalação física dos equipamentos.

- Deverá ser utilizado cabo UTP CAT6 e todos os acessórios para conexão também deverão ser certificado para CAT6.
- Todos os pontos deverão ser concentrados em um rack disponibilizado pela contratante. A contratada deverá fornecer patch panel CAT6 e acessórios para conectorização dos cabos dos AP´s no rack e fornecer patch cords CAT6 para conexão até os switches disponibilizados pela contratante.
- Todos os pontos de conexão deverão ser certificados para CAT6 com emissão de laudo individual.
- O encaminhamento dos cabos do rack até os AP´s deverá ser feito utilizando as eletrocalhas já disponibilizadas na edificação. Não serão aceitas instalações aparentes.
- Todos cabos, pontos de conexão e derivações deverão ser identificadas com etiquetas próprias para tal fim, respeitando a simbologia adotada pela DMED.

2. Detalhamento principais materiais

- Patch Panel Cat. 6
  - Carregado com guia de cabos traseiros, ícones de identificação e acessórios de fixação.
  - Canal U/UTP para conector fêmea, Patch Cord metálico e cabo eletrônico Cat. 6 23AWGx4P.
  - Altura de 44,45mm, na cor preta, com conector tipo RJ-45, com 24 posições, fabricado em material de aço / termoplástico alto impacto.
  - O fabricante preferencialmente deverá apresentar certificação ISO 9001 e ISO 14001;
  - Possuir local para aplicação de ícones de identificação (para codificação), conforme requisitos da norma ANSI/TIA/EIA-606-A, fornecido de fábrica com ícones de identificação;

2.2. Cabo U/UTP - Categoria 6 CM – Cor Azul

- Possuir certificado de performance elétrica (VERIFIED) pela UL ou ETL, conforme especificações da norma ANSI/TIA/EIA-568-B.2-1 CATEGORIA 6 e ISO/IEC 11801 bem como certificado para flamabilidade (UL LISTED ou ETL LISTED) CM conforme UL;
- O produto deve cumprir com os requisitos quanto à taxa máxima de compostos que não agridam ao meio ambiente conforme a norma RoHS;
- Ser composto por condutores de cobre sólido; capa externa em PVC não propagante à chama;
- Deve atender ao código de cores especificado abaixo:
  - par 1: azul-branco, com uma faixa azul (stripe) no condutor branco;
  - par 2: laranja-branco, com uma faixa laranja (stripe) no condutor branco;

- par 3: verde-branco, com uma faixa verde (stripe) no condutor branco;
- par 4: marrom-branco, com uma faixa marrom (stripe) no condutor branco.

- Exceder as características elétricas contidas na norma ANSI/TIA/EIA-568-B.2-1 Categoria 6;
- Impedância característica de 100Ω (Ohms);

2.3. Patch Cord Categoria 6 – Cor Azul

- Possuir Certificação UL ou ETL LISTED;
- Possuir Certificação ETL VERIFIED;
- Deve cumprir com os requisitos quanto à taxa máxima de compostos que não agridam ao meio ambiente conforme a norma RoHS;
- Deverão ser montados e testados em fábrica, com garantia de performance;
- O acessório deve ser confeccionado em cabo par trançado, U/UTP Categoria 6 (Unshielded Twisted Pair), 23 AWG x 4 pares, composto por condutores de cobre flexível, multifilar, isolamento em poliolefina e capa externa em PVC não propagante a chama, conectorizados à RJ-45 macho Categoria 6 nas duas extremidades, estes conectores (RJ-45 macho), devem atender às especificações contidas na norma ANSI/TIA/EIA-568-B.2-1 Categoria 6, ter corpo em material termoplástico de alto impacto não propagante a chama que atenda a norma UL 94 V-0 (flamabilidade), possuir vias de contato produzidas em bronze fosforoso com camadas de 2,54 μm de níquel e 1,27 μm de ouro, para a proteção contra oxidação, garras duplas para garantia de vinculação elétrica com as veias do cabo;
- Deve possuir classe de flamabilidade no mínimo CM;
- O Cabo utilizado deve apresentar Certificação ETL em conformidade com a norma ANSI/TIA/EIA-568-B.2-1 CATEGORIA 6 (stranded cable);
- Deve possuir capa protetora (bota) do mesmo dimensional do RJ-45 plug e proteção à lingueta de travamento. Esta capa protetora deve ajudar a evitar a curvatura excessiva do cabo em movimentos na conexão bem como proteger o pino de destravamento dos conectores contra enroscamentos e quebras;
- Exceder as características elétricas contidas na norma ANSI/TIA/EIA-568-B.2-1 Categoria 6;
- Possuir características elétricas e performance testada em freqüências de até 250 MHz;
- O fabricante preferencialmente deverá apresentar certificação ISO 9001 e ISO 14001.
- Deve ser fornecido com certificação emitida pelo próprio fabricante na categoria CAT6;
- Comprimento de 1,5 metros.

2.4. Conector RJ-45 Fêmea - Categoria 6

- Possuir certificações Listed pela UL ou ETL;
- Possuir certificação de canal para 6 conexões emitido pelos laboratórios reconhecidos internacionalmente (UL e ETL);
- Fornecido com instrução de montagem na língua Portuguesa;
- Apresentar disponibilidade de fornecimento nas cores: branco, bege, cinza, vermelho, azul, amarelo, marrom, laranja, verde e preto;
- O produto deve cumprir com os requisitos quanto à taxa máxima de compostos que não agridam ao meio ambiente conforme a norma RoHS.
- Possuir terminação do tipo 110 IDC (conexão traseira) estanhados, permitir inserção de condutores de 22 AWG a 26 AWG, deve garantir a presença de banho de níquel de 100um e banho de ouro de 50um nas vias de contato do RJ-45.

- Faz parte integrante deste anexo, arquivo contendo a planta-baixa do prédio da DMED, com a área de cobertura do Wi-Fi hachurada. O conjunto de pontos de acesso deverá atender toda área hachurada de maneira satisfatória, sem a presença de áreas de sombra. Para verificação de conectividade utilizaremos um celular padrão conectado na rede a ser implantada.

- **Garantia dos produtos**: O prazo mínimo de garantia é de 03 (três) anos

- Maiores informações e esclarecimentos referentes às especificações dos materiais, favor contatar o Sr. Eduardo de Souza, pelo e-mail esouza@dmedsa.com.br, com cópia para a pregoeira para o e-mail efelipe@dmedsa.com.br.