ANEXO II – REQUISITOS TÉCNICOS DA SOLUÇÃO
Pregão Eletrônico nº __/2022 – Processo Administrativo nº 1946/2022

1. CONTRATAÇÃO DE SOLUÇÃO REDE SEM FIO

1.1. DESCRIÇÃO DO OBJETO

A solução de rede sem fio será composta de:

- 24 pontos de acesso 802.11ax - Wifi 6;
- Solução de gerenciamento centralizado;
- Serviços de instalação e configuração;
- Capacitação;
- Garantia e suporte.

1.2. PONTOS DE ACESSO

- 24 equipamentos (2x2 MU-MIMO).
- Os pontos de acesso deverão possuir certificado emitido pelo *WIFI Alliance* comprovando os seguintes padrões, protocolos e funcionalidades:
    - IEEE 802.11a;
    - IEEE 802.11b;
    - IEEE 802.11g;
    - IEEE 802.11n;
    - IEEE 802.11ac;
    - Wi-Fi CERTIFIED 6;
    - WPA2 Enterprise/Personal;
    - WPA3 Enterprise/Personal;
    - WMM;
    - Short Guard Interval (SGI);
    - Packet Aggregation (A-MPDU);
    - Operar simultaneamente em 2.4GHz e 5GHz;
    - Operar com canais de 40MHz e 80MHz para a frequência de 5GHz.
- Deve implementar funcionamento em modo gerenciado por controlador WLAN, para configuração de seus parâmetros de rede sem fio, gerenciamento das políticas de segurança, QoS e monitoramento de RF;
- O ponto de acesso poderá estar diretamente ou remotamente conectado ao controlador WLAN, inclusive via roteamento da camada de rede OSI;
- Se um controlador WLAN falhar, os pontos de acesso relacionados deverão se associar automaticamente a um controlador WLAN alternativo, não permitindo que a rede sem fio se torne inoperante;
- Implementar mecanismo de funcionamento para trabalhar com controladores WLAN em redundância;
- Deve implementar funcionamento em modo auto-gerenciado, sem necessidade de controladora WLAN para configuração de seus parâmetros de rede sem fio, gerenciamento das políticas de segurança, QoS e monitoramento de RF. Deve obedecer à todas as características descritas mesmo neste modo de funcionamento;

- O ponto de acesso deve permitir a conversão de modo auto-gerenciado para modo gerenciado através de interface gráfica, em *browser* padrão (HTTPS);
- No modo de funcionamento auto-gerenciado deve disponibilizar na interface gráfica informações de usuários conectados, qualidade de sinal e tráfego de dados na rede.
- Em modo auto-gerenciado:
    - Deve permitir que o conjunto de pontos de acesso sejam atualizados de forma centralizada pela interface gráfica;
    - Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior.
- Possibilitar *backup* e restauração da configuração através da interface gráfica;
- Deve possuir servidor DHCP interno;
- Possuir capacidade de identificação e listagem dos rádios vizinhos e respectivos SSID/BSSID;
- Implementar associação dinâmica de usuários à VLANs com base nos parâmetros da etapa de autenticação;
- Deve possuir uma base de usuários interna que diferencie usuários visitantes de funcionários, para ser usada em autenticação 802.1x ou *captive portal*;
- Permitir a autenticação para acesso dos usuários conectados nas redes WLAN através de: MAC Address, 802.1x em base Local, *captive portal*, 802.1x em base externa RADIUS ou 802.1x em base externa LDAP;
- Deve permitir a seleção/uso de servidor de autenticação específico com base no SSID;
- Deve permitir, simultaneamente, usuários configurados nos padrões IEEE 802.11b, 802.11g, 802.11a, 802.11n, 802.11ac e 802.11ax;
- Implementar as seguintes taxas de transmissão e com *fallback* automático:
    - IEEE 802.11 a/g: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps;
    - IEEE 802.11 b: 11; 5,5; 2 e 1 Mbps;
    - IEEE 802.11n (2.4GHz): MCS0 – MCS15 (6.5 a 300Mbps);
    - IEEE 802.11ac (5GHz): MCS0 – MCS9, NSS = 1 a 2 (6.5 a 867 Mbps);
    - IEEE 802.11ax (2.4GHz): MCS0 – MCS11, NSS = 1 a 2 (3.6 a 574 Mbps);
    - IEEE 802.11ax (5GHz): MCS0 – MCS11, NSS = 1 a 2 (3.6 a 1.201 Mbps);
- Deve implementar multi-user MIMO (MU-MIMO);
- A potência de transmissão deve permitir ajuste em intervalos de 0,5 dBm;
- Possuir capacidade de selecionar automaticamente o canal de transmissão;
- Permitir o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar o tamanho da célula de RF;
- Possuir suporte a pelo menos 16 SSIDs;
- Permitir habilitar e desabilitar a divulgação do SSID;
- Implementar diferentes tipos de combinações encriptação/autenticação por SSID;
- Implementar padrão WMM da *Wi-Fi Alliance* para priorização de tráfego, suportando aplicações em tempo real, tais como, VoIP, vídeo, dentre outras;
- Não deve haver licença restringindo o número de usuários por ponto de acesso;
- Possuir antenas compatíveis com as frequências de rádio dos padrões IEEE 802.11a/n/ac/ax e 802.11/b/g/n com ganho de, pelo menos, 4.2 dBi, com padrão de irradiação omnidirecional;
- Suportar operação em no mínimo 2x2 MIMO;
- Possuir potência máxima de transmissão de, no mínimo, 21 dBm para IEEE 802.11a/b/g/n/ac/ax;
- Deve possuir sensibilidade de recepção de valor menor ou igual: a -93 dBm a 6Mbps no padrão 802.11g; e a -75 dBm a 54Mbps no padrão 802.11a;

- Implementar VLANs conforme padrão IEEE 802.1Q;
- Deve possuir uma interfaces Ethernet, sendo:
    - 01 interface no padrão IEEE 802.3 10/100/1000Base-T RJ45 Ethernet, auto-sensing, auto MDI/MDX;
- Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces *ethernet* ou serial (terminal assíncrono);
- Possuir porta de console para gerenciamento e configuração via linha de comando CLI com conector RJ-45, conector padrão RS-232 ou USB;
- Deve possuir radio *bluetooth* ou BLE no equipamento;
- Possuir ferramentas de *debug* e *log* de eventos para depuração e gerenciamento em primeiro nível;
- Implementar cliente DHCP, para configuração automática de rede;
- Deve configurar-se automaticamente ao ser conectado na rede;
- Possuir LED's indicativos do estado de operação, da atividade do rádio e da interface *ethernet*;
- Possibilitar alimentação elétrica local e via padrão PoE+ (IEEE 802.3at);
- Possuir estrutura que permita fixação do equipamento em teto e parede e fornecer acessórios para que possa ser feita a fixação;
- Deve ser acompanhado de todos os acessórios necessários para operacionalização do equipamento, tais como: *softwares*, documentação técnica e manuais (podendo ser em CD-ROM) que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento;
- Deve implementar firewall interno à solução;
- Implementar varredura de RF nas bandas 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, para identificação de Pontos de Acesso intrusos não autorizados (rogues) e interferências no canal habilitado ao ponto de acesso e nos demais canais configurados na rede WLAN, sem impacto no seu desempenho;
- Implementar IEEE 802.1x;
- Permitir a integração com RADIUS Server com suporte aos métodos EAP citados;
- Implementar protocolo de autenticação para controle do acesso administrativo ao equipamento com mecanismos de AAA;
- Implementar criptografia do tráfego local;
- Implementar WPA com algoritmo de criptografia TKIP e MIC;
- Implementar WPA2 com algoritmo de criptografia AES, 128/256 bits, IEEE 802.11i;
- A garantia do ponto de acesso sem fio indoor descrito neste item, deverá ser comprovada atráves de declaração expressa em carta oficial do fabricante;
- Deve possuir garantia por 60 meses do fabricante a qual dever ser comprovada mediante documento oficial do fabricante;
- Os serviços serão solicitados mediante a abertura de um chamado efetuado por técnicos da contratante, via chamada telefônica local, a cobrar ou 0800, *e-mail*, *website* ou chat do fabricante;
- Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante do *software* de gerência deste termo de referência.

1.3. SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO

Características gerais da licença:

- A licença deve ser fornecida para gerenciar 1 dispositivo de rede (ponto de acesso sem fio);
- A licença deve ser compatível com pontos de acesso sem fio, conforme suas características descritas neste termo de referência;
- As licenças deverão ser acompanhadas de garantia do fabricante para o período de 60 (sessenta) meses;

Características gerais do *software* de gerenciamento, quando licença aplicada em ponto de acesso:

- A solução de gerência de rede deve ser fornecida em *appliance* virtual ou físico;
- Deve ser obrigatoriamente do mesmo fabricante dos pontos de acesso deste certame;
- Deve permitir a configuração e gerenciamento através de *browser* padrão (HTTP, HTTPS);
- Deve possuir mecanismo incorporado para descoberta de redes (*network discovery*);
- Deve permitir o controle de acesso de usuário ao NMS através de regras administrativas (somente leitura, leitura/escrita);
- Deve permitir que os eventos sejam gravados remotamente utilizando *syslog*;
- Deve ser aprovado e certificado por entidade pública para garantia de segurança na comunicação;
- Deve permitir a visualização de alertas da rede em tempo real (*real-time*);
- Deve permitir a visualização da topologia com mapeamento automatizado;
- Suportar no mínimo um dos métodos citados: SSH, HTTP/HTTPS, SSL;
- Deve possuir ferramentas de *debug* e *log* de eventos para depuração e gerenciamento em primeiro nível;
- Prover organização hierárquica de equipamentos, permitindo que um equipamento receba as configurações lógicas e as replique a outros equipamentos;
- Possuir capacidade de projeto automatizado de redes sem fio nos padrões 802.11a, 802.11b e 802.11g, 802.11n, 802.11ac, 802.11ax, segundo a geografia do prédio (planta);
- Considerar a área de cobertura e a banda por usuário desejada;
- Permitir a visualização de alertas da rede em tempo real;
- Permitir a visualização de eventuais áreas sem cobertura de RF (áreas de sombra);
- Monitorar o desempenho da rede, consolidando informações de rede;
- Possuir capacidade de configuração gráfica completa dos Itens constantes neste termo de referência;
- Deve permitir autenticação de usuários através de base local e também através de TACACS+, RADIUS e LDAP;
- Deve implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de *traps*;
- Permitir a administração centralizada dos AP's sem a necessidade de configurar os mesmos individualmente;
- Possibilitar a importação de plantas baixas em pelo menos um dos formatos gráficos (cad, dwg, jpg, gif, png);
- Deve possuir informação sobre possíveis ameaças à rede detectadas pelos sistemas gerenciados;

- Deve possibilitar criação de regras de detecção de ameaças e correlacionar todos os dispositivos gerenciados;
- Deve possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;
- Deve possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória, etc.;
- Deve permitir a administração centralizada dos pontos de acesso sem fio sem a necessidade de configurar equipamentos individualmente;

Controle de acesso à rede sem fio (*captive portal*)

- Deve realizar a autenticação de usuários e seus dispositivos para controle de acesso à rede baseada em página ou formulário preenchido via internet (*captive portal*);
- Deve suportar integração com bases de dados de usuários do tipo LDAP;
- Deve suportar autenticação baseada em endereço MAC;
- Deve suportar protocolo RADIUS;
- Realizar consultas em bancos de dados (PostgreSQL) e LDAP, com o objetivo de buscar informações a serem utilizadas durante o processo de autenticação dos usuários;
- Gerenciar a autenticação de usuários e dispositivos de forma centralizada, permitindo a autenticação através dos seguintes métodos:
    - Base local presente na plataforma de gerência;
    - Externa via RADIUS;
    - Externa via LDAP/Microsoft Active Directory.
- Suporte às seguintes bases de dados:
    - Base SQL interna;
    - Microsoft Active Directory;
    - LDAP;
    - Bancos de dados (PostgreSQL);
- Permitir a visualização de todas as informações relativas a cada transação/autenticação em uma única tela, como data e hora, endereço mac do dispositivo, classificação do dispositivo, usuário, equipamento que requisitou a autenticação (origem), método de autenticação utilizado, fonte de autenticação utilizada para validação, perfil de acesso aplicado, todos atributos de entrada do protocolo utilizado na requisição (ex. RADIUS), informações de resposta da solução para o elemento de rede, alertas em caso de falha, exibição de logs já filtrados para a requisição em análise;
- Deve suportar autenticações via OAuth2, Facebook, Twitter, LinkedIn, Office365 e Google Apps;
- Possuir recursos integrados de AAA: RADIUS, TACACS+;
- Suporte a RADIUS Web authentication e SAML v2.0;
- Suporte à integração com plataforma de terceiros usando HTTP/RESTful API;
- Suporte a administração através de IPv6;
- Características das funções de *guest* (visitantes):
    - Deve permitir a otimização do portal de visitantes para *desktops*, *tablets*, *smartphones*, *notebooks* e *laptops*, ou seja, ser adaptativo conforme o tipo de dispositivo conectado;
    - Deve permitir a customização do portal de visitantes;
    - Deve possuir ferramenta para gerenciar os processos de credenciamento, autenticação, autorização e contabilidade de usuários visitantes através de um portal *web* seguro;

- Deve realizar a autenticação dos autorizadores em base externa do tipo Microsoft Active Directory ou LDAP;
- Deve implementar a importação e exportação da relação de credenciais temporárias (*vouchers* de acesso) através de arquivos txt ou csv;
- Deve permitir a determinação da validade das credenciais, pela escolha de um dos critérios a seguir: validade previamente determinada, criação da conta e após o primeiro login da conta;
- Deve permitir o gerenciamento das credenciais de visitantes;
- Deve permitir a configuração de contas de usuários visitantes com as seguintes características: Prazo de validade, largura de banda;
- Deve permitir a criação e gerenciamento de múltiplas contas de usuários visitantes;
- Deve prover meios de impedir o acesso à rede de visitante;
- Deve possuir recursos para detecção automática do idioma do dispositivo do visitante para que a página virtual com o formulário de autenticação seja apresentada no mesmo idioma;
- Deve permitir que o visitante altere sua própria senha utilizando-se do portal *web*;
- Deve permitir que o visitante crie sua própria credencial temporária ("*self-service*") através do portal *web*, sem a necessidade de um autorizador;
- Deve permitir a customização do formulário de criação de credenciais, a ser preenchido pelo autorizador ou pelo visitante, em caso de auto-serviço, especificando quais informações cadastrais dos visitantes são obrigatórias ou opcionais;
- Deve permitir a customização do nível de segurança da senha temporária que será gerada ao visitante, especificando a quantidade mínima de caracteres e o uso de caracteres especiais, números e letras para compor a senha;
- Deve permitir configuração para que o usuário visitante precise aceitar o texto com o "Termo de uso da rede sem fio" mostrado em cada *login* e alternativamente apenas no primeiro login para ganhar acesso a rede;
- Deve permitir o envio das credenciais aos usuários registrados através de mensagens SMS email e impressão local;
- Deve permitir a utilização de recurso do tipo *captcha* no *captive portal*;
- Desejável possibilitar serviço de, por exemplo, exibir vídeo antes de liberar o acesso;
- Deve permitir o *login* automático de usuários que realizem o auto-registro;
- Deve permitir a desconexão de múltiplas sessões ativas;
- Deve possuir página que exibe estatística de sessão após realizar login.

- Todas licenças necessárias para o atendimento das funcionalidades solicitadas nesta especificação deverão ser fornecidas;
- Todas licenças deverão ser preferencialmente permanentes e perpétuas. Em caso de licenças do tipo subscrição deverão ser fornecidas por um período mínimo de 5 anos;
- Deve permitir realizar atualizações de versão do sistema para correção de *bugs* de *software* e atualizações de segurança;

1.4. SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO

Serviço de *Assessment* e Planejamento

- O serviço de assessment e planejamento compreende o diagnóstico inicial e avaliação do ambiente;
- Ele compreende, mas não se limita à: atividades de revisão de topologia, análise de rede, dentre outros e pontua-se como item de requisito para o dimensionamento da infraestrutura futura;

- O resultado da análise deve compreender os planos de revisão e instalação a serem disponibilizados;
- O esforço e todas as atividade necessárias ao dimensionamento deverão ser executadas por equipe dedicada a essa finalidade sob responsabilidade da CONTRATADA e deverá contar com o acompanhamento da equipe técnica da CONTRATANTE;
- A avaliação do ambiente (assessment e planejamento) da rede deverão ser executados em local definido pela CONTRATANTE, através de prévio agendamento;
- Todas as despesas com ferramental necessário, alimentação, deslocamento e demais itens relacionados à entrega dos serviços dessa finalidade deverão ser de responsabilidade da CONTRATADA;
- Deverá ser realizada uma reunião prévia com a participação da equipe técnica da CONTRATANTE e da CONTRATADA para alinhamento de expectativas em relação às atividades a serem executadas, explanação dos trâmites identificados e apresentação dos planos os quais deverão ser apresentados, discutidos e aprovados;
- Como referência para o planejamento e execução das atividades e como resultado deverão ser produzidos e entregues pela CONTRATADA, no mínimo, os seguintes documentos:
    - Plano de instalação/readequação, composto por:
        - Atividades a serem realizadas;
        - Cronograma estimado;
        - Quantidade de horas para execução das atividades;
        - Atividades extras, quando aplicável.

  Serviços de instalação, readequação e suporte:
- O pacote compreende os recursos técnicos necessários para a execução dos serviços especializados para:
    - A instalação, quando se referir a ações de configuração inicial de algum componente necessário e exigido, desde que se tenha referência e esteja presente na relação dos itens de entrega deste processo de licitação;
    - Readequação, quando se referir a ações de ajustes e intervenções técnicas em itens já existentes na infraestrutura legada da CONTRATANTE; não se aplicando quando demandar substituição de *hardware* ou troca de peças;
    - Suporte, quando se referir a esclarecimento de dúvidas, ações pontuais de diagnósticos, apoio e revisão de configuração e remetem ao período contratado e que tenham relação com a instalação dos itens do objeto desse documento;
- Os serviços deverão ser executados na sua totalidade pela CONTRATADA e deverão ter o acompanhamento da equipe técnica da CONTRATANTE.
- Exige-se que o acompanhamento seja desempenhado por profissional que detenha conhecimento técnico a respeito da topologia de rede e disponha das credenciais de administração necessárias;
- Instalação, readequação ou suporte deverão ser executados no local definido pela CONTRATANTE, mediante prévio agendamento;
- Deverá ser de responsabilidade da CONTRATADA todas as despesas decorrentes com a alimentação, deslocamentos, transporte, estadia e demais itens relacionados à entrega dos serviços;
- Durante a execução das atividades de instalação e implantação, até a sua conclusão com os testes finais de homologação e aceite, poderão ser realizadas reuniões periódicas de acompanhamento com a área técnica do CONTRATANTE para acompanhamento e eventuais ajustes no projeto;
- O escopo de atividades do referido item, será executado conforme documento de planejamento apresentado pela CONTRATADA elaborado no item Serviço de Assessment e Planejamento;

- Como referência para o planejamento e execução das atividades, deverão ser produzidos e entregues pela CONTRATADA, no mínimo, os seguintes documentos:
    - Escopo Instalação
        - Descrição do escopo da solução, composta por detalhes da implantação, os trâmites necessários e intervenções a serem conduzidas de forma a integrar os recursos contratados ao ambiente computacional do CONTRATANTE;
        - Desenho da arquitetura física da solução, detalhando todas as conexões físicas e interligações entre os ativos da solução e o ambiente computacional do CONTRATANTE, com destaques para as informações de portas e endereços, em formato gráfico e composto por legendas que explanem os itens que irão compor a solução;
    - Plano de Configuração e Integração
        - Detalhando as especificações necessárias para a implantação dos serviços – instalação, configuração e integração de todos os produtos com o ambiente operacional do CONTRATANTE;
    - Plano de Homologação e Testes
        - Descrevendo todo o processo a ser realizado a fim de que se atenda aos requisitos mínimos exigidos para homologação e aceite final dos produtos e serviços, detalhando testes e atividades a serem executadas para validar a solução após a sua implantação.