ESTUDO TÉCNICO PRELIMINAR (Res. CNJ 182/2013)

Demanda: Aquisição de Equipamentos para Rede sem fio (WIFI), para ampliação da rede existente e substituição de equipamentos que estão apresentando problemas.
Processo nº 4561/2021

São Luís, 2021

Em atendimento à Resolução nº 182 de 17/10/2013 que regulamenta as diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação (STIC) realizadas pelos órgãos submetidos ao controle administrativo e financeiro do CNJ

Equipe de Planejamento:

Leonardo Araujo Sousa
Matrícula 129.502
Chefe da Divisão
de Administração de Redes

Leonardo Araújo Sousa
Mat 129502

José Eduardo Carvalho Thomaz
Mat 129437

São Luís (MA)

abril/2021

1. APRESENTAÇÃO

Fundamentos e Diretrizes dos Estudos Preliminares

O presente estudo buscou a observância do §1o do art. 12 da Resolução no 182/2013 do Conselho Nacional de Justiça (CNJ), que determina que os Estudos Preliminares da área de TIC deverão contemplar as seguintes etapas:

I – Análise de Viabilidade da Contratação;
II – Sustentação do Contrato;
III – Estratégia para a Contratação; e
IV – Análise de Riscos.

Após a contextualização da demanda, seguem os documentos integrantes do estudo técnico preliminar realizado, nos termos definidos nos arts. 14 a 17 da supracitada Resolução.

Contextualização

A presente demanda justifica-se pela necessidade de ampliação da Rede e substituição de equipamentos que estão apresentando problemas, impactando negativamente na performance e disponibilidade da rede WIFI nos prédios que integram o PJMA.

Atualmente o TJMA conta com redes de comunicação sem fio em boa parte dos seus prédios. No entanto, essas redes não contam com equipamentos e sistemas que garantam a autenticação e segurança no acesso aos dados disponibilizados por essas redes, tornando-as vulneráveis à usuários maliciosos.

Esta nova contratação é importante para o TJMA, pois visa dar mais segurança no acesso às redes sem fio, além de possibilitar a expansão destas redes para prédios ainda não contemplados com essa tecnologia.

Este Estudo Técnico Preliminar visa atender a Resolução N° 182/2013 do CNJ (Conselho Nacional de Justiça), e tem o objetivo de analisar informações sobre a aquisição de equipamentos para adequação e expansão das redes sem fio e avaliar possíveis soluções tecnológicas para atender as demandas da Diretoria de Informática e Automação (DIA).

2. ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO (Art.14)

2.1 Descrição da Solução a ser contratada

Aquisição de Equipamentos para Rede sem fio (WIFI), para ampliação da rede existente e substituição de equipamentos que estão apresentando problemas.

2.2 Justificativa

Devido a necessidade de ampliação da Rede e substituição de equipamentos que estão apresentando problemas, impactando negativamente na performance e disponibilidade da rede WIFI nos prédios que integram o PJMA.

2.3 Definição e Especificação dos Requisitos da Demanda (Art.14, I)

2.3.1. Ponto de acesso interno – Aironet 9105

2.3.1.1. Equipamento do tipo thin access point, ou seja, ponto de acesso (AP) que permita acesso à rede ethernet via wireless e que possua todas as suas configurações centralizadas nas controladoras wireless;

2.3.1.2. Hardware/unidade projetada com estrutura robusta, com facilidades para fixação em parede ou teto e capaz de operar em ambiente de escritório. Deve acompanhar todos os acessórios para fixação em teto e/ou parede. Temperatura de operação de 5 a 50º C;

2.3.1.3. O AP deve suportar arquitetura centralizada onde opera de modo dependente do controlador wireless que faz o gerenciamento das políticas de segurança, qualidade de serviço (QoS) e monitoramento de RF, utilizando para isto o protocolo de gerenciamento de RF específico;

2.3.1.4. As funcionalidades aqui descritas devem ser implementadas pelo conjunto ponto de acesso + controladores;

2.3.1.5. Deve implementar padrões IEEE 802.11a/b/g/n/ac/ax simultaneamente com rádios distintos, permitindo configurações distintas para 2.4 e 5 GHz dentro do mesmo equipamento;

2.3.1.6. Suporte integrado a Power Over Ethernet (PoE) conforme o padrão IEEE 802.3af ou 802.3at;

2.3.1.7. Deve suportar no mínimo 16 (dezesseis) SSIDs com configurações distintas de rede, VLAN, segurança, criptografia e QoS. Deve ser possível habilitar todos os 16 (dezesseis) SSIDs simultaneamente em uma única faixa de frequência, tanto em 2.4GHz quanto em 5GHz;

2.3.1.8. Deve possuir 01 (uma) interface Ethernet com conector RJ-45 para conexão de cabos UTP com operação nas seguintes velocidades: 100Mbps e 1Gbps;

2.3.1.9. Deve possuir 01 (uma) interface console (serial) para gerenciamento local;

2.3.1.10. Deve possuir potência mínima de 100 mW em ambas as frequências. Não serão aceitos equipamentos com potência inferior;

2.3.1.11. Deve possuir LED com intuito de obter-se o status do equipamento;

2.3.1.12. Deve possibilitar configuração inicial através de cliente DHCP, de modo que toda configuração seja baixada do controlador automaticamente;

2.3.1.13. Implementar gerenciamento automatizado de RF e potência, ou seja, os elementos da solução (Controlador + AP) devem definir sem intervenção manual os parâmetros de potência de transmissão e ajuste de canal de frequência, evitando interferências e sobreposição de canais;

2.3.1.14. Deve suportar operação MU-MIMO (multiuser MIMO) em 2x2 e com 2 fluxos espaciais;

2.3.1.15. Deve possuir antenas internas ao equipamento com ganho mínimo de 4 dBi em 2.4 GHz e 5 dBi em 5 GHz. As antenas devem possuir radiação omnidirecional;

2.3.1.16. Deve implementar a utilização de canais de 80MHz em 802.11ac/ax;

2.3.1.17. Para segurança, o AP deve suportar o padrão IEEE 802.11i e suportar autenticação WPA3. O AP também deve suportar autenticação 802.1x incluindo EAP-TLS, EAP-TTLS, EAP-GTC, EAP-SIM e PEAP. O AP deve suportar o algoritmo AES para criptografia;

2.3.1.18. Suportar autenticação segundo o padrão IEEE 802.1X com assinalamento de VLAN por usuário, conforme pré-definido em servidor RADIUS padrão de mercado (tais como NPS e FreeRADIUS);

2.3.1.19. Deve implementar técnica de beamforming de forma nativa;

2.3.1.20. Deve implementar técnica de DFS (Dynamic Frequency Selection);

2.3.1.21. Deve implementar OFDMA e BSS coloring;

2.3.1.22. Deve acompanhar licença para adicioná-lo ao controlador virtual especificado neste Termo de Referência;

2.3.1.23. Deve acompanhar 01 (uma) licença do tipo token para permitir adição de dispositivos no software de gerenciamento Cisco Prime Infrastructure existente na contratante;

2.3.1.24. Deverá ser do mesmo fabricante e compatível com o software de gerenciamento Cisco Prime atualmente instalado no tribunal;

2.3.1.25. O equipamento fornecido não pode constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support, end-of-engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo

estar em linha de produção do fabricante. Também não serão aceitos equipamentos usados, remanufaturados ou de demonstração.

2.3.1.26. Garantia de 60 (sessenta) meses com cobertura pelo fabricante no Brasil;

2.3.2. Ponto de acesso interno - Aironet 9115

2.3.2.1. Equipamento do tipo thin access point, ou seja, ponto de acesso (AP) que permita acesso à rede ethernet via wireless e que possua todas as suas configurações centralizadas nas controladoras wireless;

2.3.2.2. Hardware/unidade projetada com estrutura robusta, com facilidades para fixação em parede ou teto e capaz de operar em ambiente de escritório. Deve acompanhar todos os acessórios para fixação em teto e/ou parede. Temperatura de operação de 5 a 50º C;

2.3.2.3. O AP deve suportar arquitetura centralizada onde opera de modo dependente do controlador wireless que faz o gerenciamento das políticas de segurança, qualidade de serviço (QoS) e monitoramento de RF, utilizando para isto o protocolo de gerenciamento de RF específico;

2.3.2.4. As funcionalidades aqui descritas devem ser implementadas pelo conjunto ponto de acesso + controladores;

2.3.2.5. Deve implementar padrões IEEE 802.11a/b/g/n/ac/ax simultaneamente com rádios distintos, permitindo configurações distintas para 2.4 e 5 GHz dentro do mesmo equipamento;

2.3.2.6. Suporte integrado a Power Over Ethernet (PoE) conforme o padrão IEEE 802.3af ou 802.3at;

2.3.2.7. Deve suportar no mínimo 16 (dezesseis) SSIDs com configurações distintas de rede, VLAN, segurança, criptografia e QoS. Deve ser possível habilitar todos os 16 (dezesseis) SSIDs simultaneamente em uma única faixa de frequência, tanto em 2.4GHz quanto em 5GHz;

2.3.2.8. Deve possuir 01 (uma) interface Ethernet com conector RJ-45 para conexão de cabos UTP com operação nas seguintes velocidades: 100Mbps, 1Gbps e 2,5Gbps;

2.3.2.9. Deve possuir 01 (uma) interface console (serial) para gerenciamento local;

2.3.2.10. Deve possuir potência mínima de 200 mW em ambas as frequências. Não serão aceitos equipamentos com potência inferior;

2.3.2.11. Deve possuir LED com intuito de obter-se o status do equipamento;

2.3.2.12. Deve possibilitar configuração inicial através de cliente DHCP, de modo que toda configuração seja baixada do controlador automaticamente;

2.3.2.13. Implementar gerenciamento automatizado de RF e potência, ou seja, os elementos da solução (Controlador + AP) devem definir sem intervenção manual os parâmetros de potência de transmissão e ajuste de canal de frequência, evitando interferências e sobreposição de canais;

2.3.2.14. Deve suportar operação MU-MIMO (multiuser MIMO) em 4x4 e com 4 fluxos espaciais;

2.3.2.15. Deve possuir antenas internas ao equipamento com ganho mínimo de 3 dBi em 2.4 GHz e 4 dBi em 5 GHz. As antenas devem possuir radiação omnidirecional;

2.3.2.16. Deve implementar a utilização de canais de 160MHz em 802.11ac/ax;

2.3.2.17. Para segurança, o AP deve suportar o padrão IEEE 802.11i e suportar autenticação WPA3. O AP também deve suportar autenticação 802.1x incluindo EAP-TLS, EAP-TTLS, EAP-GTC, EAP-SIM e PEAP. O AP deve suportar o algoritmo AES para criptografia;

2.3.2.18. Suportar autenticação segundo o padrão IEEE 802.1X com assinalamento de VLAN por usuário, conforme pré-definido em servidor RADIUS padrão de mercado (tais como NPS e FreeRADIUS);

2.3.2.19. Deve implementar técnica de beamforming de forma nativa;

2.3.2.20. Deve implementar técnica de DFS (Dynamic Frequency Selection);

2.3.2.21. Deve implementar OFDMA e BSS coloring;

2.3.2.22. Deve acompanhar licença para adicioná-lo ao controlador virtual especificado neste Termo de Referência;

2.3.2.23. Deve acompanhar 01 (uma) licença do tipo token para permitir adição de dispositivos no software de gerenciamento Cisco Prime Infrastructure existente na contratante;

2.3.2.24. Deverá ser do mesmo fabricante e compatível com o software de gerenciamento Cisco Prime atualmente instalado no tribunal;
2.3.2.25. O equipamento fornecido não pode constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support, end-of-engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante. Também não serão aceitos equipamentos usados, remanufaturados ou de demonstração.
2.3.2.26. Garantia de 60 (sessenta) meses com cobertura pelo fabricante no Brasil

2.3.3. Ponto de acesso externo – Aironet 1562i

2.3.3.1. Hardware/unidade projetada com estrutura robusta, lacrada, sem espaços para problemas com poeira, umidade, água e chuva, com facilidades para fixação em poste, capaz de operar em ambiente outdoor. Deve acompanhar todos os acessórios para fixação em poste e parede;
2.3.3.2. Deve possuir grau de proteção IP67 e suportar temperatura de operação de 0 a 55o C;
2.3.3.3. Deve possuir resistência para ventos de até 150Km/h;
2.3.3.4. O AP deve suportar arquitetura centralizada onde opera de modo dependente do controlador wireless que faz o gerenciamento das políticas de segurança, qualidade de serviço (QoS) e monitoramento de RF, utilizando para isto o protocolo de gerenciamento de RF específico;
2.3.3.5. As funcionalidades aqui descritas devem ser implementadas pelo conjunto ponto de acesso e controladoras;
2.3.3.6. Deve implementar padrões IEEE 802.11a/b/g/n/ac simultaneamente com rádios distintos, permitindo configurações distintas para 2.4 e 5 GHz dentro do mesmo equipamento;
2.3.3.7. Deve suportar no mínimo 16 (dezesseis) SSIDs com configurações distintas de rede, VLAN, segurança, criptografia e QoS. Deve ser possível habilitar todos os 16 (dezesseis) SSIDs simultaneamente em uma única faixa de frequência, tanto em 2.4GHz quanto em 5GHz;
2.3.3.8. Deve possuir 01 (uma) interface Ethernet 100/1000 com conector RJ-45 para conexão de cabos UTP;
2.3.3.9. Deve possuir 01 (uma) interface console (serial) para gerenciamento local;
2.3.3.10. Deve possuir 01 (um) slot SFP para conexão de transceiver de fibra óptica monomodo ou multimodo;
2.3.3.11. Deve possuir potência mínima de 150 mW em ambas as frequências. Não serão aceitos equipamentos com potência inferior;
2.3.3.12. Deve possuir LED com intuito de obter-se o status do equipamento;
2.3.3.13. Deve possibilitar configuração inicial através de cliente DHCP, de modo que toda configuração seja baixada do controlador automaticamente;
2.3.3.14. Implementar gerenciamento automatizado de RF e potência, ou seja, os elementos da solução (Controlador + AP) devem definir sem intervenção manual os parâmetros de potência de transmissão e ajuste de canal de frequência, evitando interferências e sobreposição de canais;
2.3.3.15. Deve possuir sensibilidade mínima de -90 dBm operando em IEEE 802.11n (2.4GHz);
2.3.3.16. Deve possuir antenas internas ao equipamento com ganho mínimo de 4 dBi em 2.4 GHz e 4 dBi em 5 GHz. As antenas devem possuir radiação omnidirecional;
2.3.3.17. Deve suportar operação com data rate de 1.3 Gbps e 3 fluxos espaciais (spatial streams);
2.3.3.18. Deve suportar operação com MIMO 3x3 (SU-MIMO e MU-MIMO);
2.3.3.19. Deve implementar análise de espectro para detecção de interferências provenientes de outros equipamentos nas frequências de 2.4 e 5GHz com granularidade melhor que 400 kHz, com chipset ou hardware dedicado para esta funcionalidade. Deve detectar interferências que operem nas frequências relacionadas, tais como bluetooth, micro câmeras, microondas, telefones sem fio e qualquer outro dispositivo que possua transmissão nestas faixas de frequências. Estas interferências devem ser evitadas pelo conjunto access point + controlador de forma que sejam utilizados nos pontos de acesso os canais menos afetados pelas interferências. Esta análise deve

ocorrer simultaneamente nas frequências de 2.4 e 5 GHz no mesmo AP sem perda de conectividade ou redução no data rate para os clientes conectados;

2.3.3.20. Para segurança, o AP deve suportar o padrão IEEE 802.11i e suportar autenticação WPA2. O AP também deve suportar autenticação 802.1x incluindo EAP-TLS, EAP-TTLS, EAP-SIM e PEAP. O AP deve suportar o algoritmo AES para criptografia;

2.3.3.21. Suportar autenticação segundo o padrão IEEE 802.1X com assinalamento de VLAN por usuário, conforme pré-definido em servidor RADIUS padrão de mercado (tais como NPS e FreeRADIUS);

2.3.3.22 Deve implementar técnica de beamforming de forma nativa;

2.3.3.23. Deve implementar técnica de DFS (Dynamic Frequency Selection);

2.3.3.24. Deve suportar alimentação através Power Over Ethernet (PoE) e acompanhar injetor PoE apropriado para o equipamento. Todos os produtos devem ser do mesmo fabricante do equipamento;

2.3.3.25. Todo o conjunto de equipamento e acessórios deve ser próprio para utilização outdoor. Não serão aceitos equipamentos adaptados para utilização em caixas externas/herméticas;

2.3.3.26. Deve estar homologado pela Anatel na data do pregão;

2.3.3.27. O ponto de acesso deverá ser capaz de ser gerenciado pela controladora virtualizada da presente contratação;

2.3.3.28. Deve ser compatível com o software de gerenciamento Cisco Prime Infrastructure existente na contratante;

2.3.3.29. O equipamento fornecido não pode constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support, end-of-engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante. Também não serão aceitos equipamentos usados, remanufaturados ou de demonstração;

2.3.3.30. Garantia de 60 (sessenta) meses com com cobertura pelo fabricante no Brasil.

2.3.4. Controladora Wireless Virtual - C9800-CI

2.3.4.1. Solução de controladora wireless que gerencie de maneira centralizada os pontos de acesso (Access Points - APs) compatíveis, espalhados pela rede deste órgão;

2.3.4.2. A solução deverá ser fornecida com controladoras wireless na forma de appliance virtual;

2.3.4.3. A solução deverá ser fornecida com software apto a funcionar com todas as características solicitadas aqui neste termo de referência;

2.3.4.4. A solução deve permitir o tráfego IP, multicast e IPv6 através do controlador (camada 2);

2.3.4.5. As funcionalidades aqui descritas devem ser implementadas pelo conjunto controladora + pontos de acesso;

2.3.4.6. Deve executar o controle, configuração e gerência dos APs, bem como otimizar o desempenho e a cobertura da radiofrequência (RF) oferecido pela solução;

2.3.4.7. A solução deve suportar simultaneamente o gerenciamento de até 6000 (seis mil) AP’s;

2.3.4.8. Deve suportar pelo menos 60.000 clientes/usuários simultâneos conectados;

2.3.4.9. A solução deve controlar APs de uso interno “indoor” e de uso externo “outdoor”, permitindo estabelecer link em wireless mesh entre eles. Caso necessário, devem acompanhar licenças para habilitar tais funcionalidades para a quantidade total de pontos de acesso suportados pela controladora;

2.3.4.10. Deve possuir funcionalidade baseada em reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede identificar quais aplicações estão sendo trafegadas pelo equipamento. Caso existam, devem ser fornecidas as licenças necessárias para funcionamento desta funcionalidade com atualização da base de aplicações durante todo o período de garantia e que contemplem o funcionamento deste recurso para a capacidade máxima de pontos de acesso que podem ser gerenciados pela controladora;

2.3.4.11. A solução deve, através da técnica de DPI, reconhecer aplicações que façam uso de voz e vídeo e permitir a priorização deste tráfego com atribuição de QoS;

2.3.4.12. A solução deve ainda permitir a criação de regras para bloqueio e limite de banda das aplicações reconhecidas através da técnica de DPI que possam ser aplicadas por SSID ou grupos de usuários;

2.3.4.13. A solução deve permitir a adição de pontos de acesso que implementem análise de espectro com granularidade melhor que 400 kHz e sem impacto no tráfego de rede dos clientes. Desta maneira, a solução como um todo deve permitir o gerenciamento mais apurado no cenário RF, utilizando da melhor maneira os canais mais imunes a interferência, ruído e/ou sujeira e alertando ao administrador do sistema possíveis ações que devam ser tomadas para troubleshooting da solução;

2.3.4.14. Ajuste dinâmico de canais e potência para otimizar a cobertura de rede e performance baseado na cobertura de APs vizinhos e interferências. Deve ser possível desabilitar o ajuste de potência e ajuste de canal automático;

2.3.4.15. Deve permitir balanceamento de carga de usuários de modo automático fazendo a distribuição de usuários entre os APs próximos de forma automática e sem intervenção humana. Deve ser possível escolher em qual WLAN (SSID) será permitido executar tal ação;

2.3.4.16. Deve implementar o controle dinâmico de potência, onde o sistema dinamicamente ajusta a saída de potência dos pontos de acesso individualmente para acomodar as condições de alterações da rede;

2.3.4.17. Implementar mecanismos para detecção de pontos de acesso não autorizados (rogues) de forma integrada e automática, classificando-os como conhecidos, maliciosos/não autorizados e não classificados;

2.3.4.18. Deve ser permitido ajustar um nível de sinal mínimo (RSSI) para que o ponto de acesso rogue seja detectado e classificado automaticamente como ponto de acesso malicioso/não autorizado;

2.3.4.19. Deve ser permitido configurar o nome do SSID utilizado pelo ponto de acesso rogue para que ele seja detectado e classificado automaticamente como ponto de acesso malicioso/não autorizado;

2.3.4.20. Deve implementar recurso que evite automaticamente a conexão de usuários wireless em pontos de acesso classificados automaticamente como maliciosos/não autorizados;

2.3.4.21. Implementar opção de escritório remoto (local switching). Neste modo não é necessário que todo o tráfego seja direcionado a controladora antes de ser encaminhado ao restante da rede, sendo possível a comunicação local seja com recursos de rede (impressoras, servidores) seja com outros usuários WiFi sem o controle prévio da controladora, otimizando a conexão em caso de pontos de acesso gerenciados sobre um link remoto (internet, WAN, MPLS);

2.3.4.22. Deve operar com AP’s remotos, mesmo acessado por NAT ou através de túnel (VPN ou semelhante). Desta forma, é possível definir o IP público da controladora e fazer com que pontos de acesso remotos conectem-se automaticamente a controladora através da Internet. Em caso de falha na comunicação entre controladora e ponto de acesso, o ponto de acesso deve continuar sua operação de transferência de dados aos clientes já conectados;

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

2.3.4.24. A solução deve detectar, classificar e mitigar interferências não WiFi que impactem diretamente no funcionamento da rede em menos de 10 minutos;

2.3.4.25. Deve implementar, no mínimo, 64 (sessenta e quatro) domínios de mobilidade (SSID), permitindo configurações distintas de autenticação, QoS, criptografia, SSID e VLAN para cada domínio. Deve ser possível especificar em quais APs/Grupos de APs cada domínio será aplicado, inclusive para os APs das unidades remotas;

2.3.4.26. Para fins de controle, deve permitir a restrição da quantidade de usuários conectados em um determinado domínio de mobilidade (SSID);
2.3.4.27. Implementar os padrões IEEE 802.11h e IEEE 802.11i;
2.3.4.28. Implementar Fast BSS Transition de acordo com o padrão IEEE 802.11r para aceleração do roaming dos usuários;
2.3.4.29. Implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente pontos de acesso próximos disponíveis para roaming;
2.3.4.30. Deve suportar a adição e gerenciamento de pontos de acesso que operem no padrão WiFi 802.11ac e 802.11ax;
2.3.4.31. Deve ser possível localizar usuários de forma integrada ao software da controladora, permitindo configurar filtros baseados em endereços MAC, nome do AP (rádio) e SSID. Ao encontrar o usuário, deve ser possível obter informações tais como: aplicações acessadas, estatísticas de conexão, endereço IP (IPv4 e IPv6), nível de sinal (RSSI), endereço MAC, quantidade de tráfego consumido e nome do usuário (caso esteja logado via 802.1x ou captive portal);
2.3.4.32. Implementar o protocolo IEEE 802.1x com associação dinâmica de usuário a VLAN com base nos parâmetros da etapa de autenticação fornecidos por servidor RADIUS;
2.3.4.33. Para permitir a maior dispersão de usuários e melhoria nas condições de RF e performance nas faixas de frequência de 2.4 e 5 GHz, deve possuir funcionalidade capaz de fazer a admissão de novos usuários de acordo com sua capacidade de operação, ou seja, a controladora deve escolher sem intervenção do usuário ou administrador, em qual frequência o usuário se conectará (se 2.4 ou 5 GHz), de acordo com hardware disponível do usuário e condições de rede, independente do SSID que o usuário estará conectando-se. Deve ser possível habilitar/desabilitar tal funcionalidade;
2.3.4.34. A solução deverá implementar técnicas de beamforming de forma nativa para os padrões 802.11a/g/n/ac, sem necessidade de softwares instalados na placa de rede dos clientes wireless;
2.3.4.35. A solução deverá operar com os padrões IEEE 802.11A/B/G/N/AC/AX, com diferentes rádios de diferentes padrões, sejam rádios operando nas frequências B/G/N, A/B/G, B/G ou qualquer uma das configurações. Também deve controlar rádio mesh outdoor, de forma a atender grandes áreas externas. Devem acompanhar todas as licenças necessárias para o funcionamento conforme os itens descritos neste processo;
2.3.4.36. Deve implementar SNTP ou NTP para sincronização de tempo com outros dispositivos de rede;
2.3.4.37. Deve implementar listas de controle de acesso (ACLs) com restrições de endereço IP, tipos de protocolos, portas, QoS e direção do fluxo de dados. Deve ser possível a criação de ACL para APs conectados remotamente (modo escritório local);
2.3.4.38. Deve implementar funcionalidades de wIDS com intuito de controlar e identificar tentativas de ataques a rede WLAN. Deve implementar mecanismos contra ataques tipo Auth Flood, Deauth Flood, EAPOL Flood e Broadcast Deauth;
2.3.4.39. Autenticação, Autorização e Accounting (AAA) em servidor RADIUS;
2.3.4.40. Em parceria com o AP, deve gerenciar chaves de criptografia WPA, WPA2, WPA3, TKIP e AES;
2.3.4.41. Além das funcionalidades de criptografia, deve possuir funcionalidade de autenticação web (captive portal). Todo o mecanismo de autenticação deve ser interno a controladora (website, lista de usuários, políticas), sendo que a criação destes usuários deverá dar-se numa tela/interface diferente da tela de gerência do equipamento, permitindo que pessoas menos qualificadas possam fazer o cadastro de novos usuários. Além disso, deve ser possível especificar o tempo que um determinado usuário (login) ficará válido para ter acesso a rede através da autenticação web;
2.3.4.42. Deve permitir o cadastramento de usuários visitantes na base interna da controladora;

2.3.4.43. Deve implementar o mecanismo de mudança de autorização dinâmica para 802.1x, conhecido como RADIUS CoA (Change of Authorization) conforme RFC 3576 ou RC 5176;
2.3.4.44. Deve permitir a atualização remota do software (firmware) da controladora e do software (firmware) dos pontos de acesso (APs), mesmo quando conectado remotamente;
2.3.4.45. Administração e gerência através de navegador padrão (HTTP/HTTPS), SSH, Telnet e interface console;
2.3.4.46. Permitir a gravação de eventos em log interno e servidor syslog externo;
2.3.4.47. Implementar SNMP v2c e v3 incluindo a geração de traps;
2.3.4.48. Possuir suporte a MIB II, conforme RFC 1213;
2.3.4.49. Deve permitir que clientes IPv6 se conectem a controladora;
2.3.4.50. Deve permitir o gerenciamento da controladora e dos pontos de acesso através de IPv6;
2.3.4.51. Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação;
2.3.4.52. Deverá ser entregue software de gerenciamento gráfico que permita o gerenciamento dos pontos de acesso;
2.3.4.53. A controladora deverá ser compatível e gerenciar os pontos de acesso deste processo;
2.3.4.54. A controladora deve ser compatível e homologada para operação com VMware ESXi 6 ou superior, KVM ou Hyper-V;
2.3.4.55. A controladora deverá operar em modo de alta disponibilidade, podendo ser configurado em ativo/passivo, ou em modo N+1. Durante a falha do controlador principal, o controlador secundário deverá assumir todas as funcionalidades, sem nenhum impacto ao ambiente;
2.3.4.56. A controladora deve ser compatível com as funcionalidades VMware vMotion, VMware Snapshot e VMware Distributed Resource Scheduler (DRS), sem impacto ao funcionamento;
2.3.4.57. Garantia de 60 (sessenta) meses com cobertura pelo fabricante no Brasil.

2.3.5. Licença para Ponto de Acesso - DNA Essentials

2.3.5.1. Deve prover a expansão da quantidade de APs gerenciados pelo controlador wireless virtual deste processo;
2.3.5.2. Deve adicionar 1 APs ao número total de APs já suportados, respeitando o limite suportado pelo controlador;
2.3.5.3. Deve acompanhar todas as habilidades para pleno funcionamento;
2.3.5.4. Deve prover a expansão da quantidade de APs gerenciados pelo software de gerenciamento Cisco Prime atualmente instalado no tribunal;
2.3.5.5. Garantia de 60 (sessenta) meses com cobertura pelo fabricante no Brasil.

2.3.6. Serviço de Instalação, Configuração e Treinamento na Solução Wireless

2.3.6.1. Os serviços devem ser executados e planejados por técnicos certificados em gerenciamento de projetos, e Wireless. Fica a cargo deste órgão a solicitação da comprovação das certificações dos técnicos responsáveis pela realização dos serviços;
2.3.6.2. Antes de iniciar a instalação e configuração da solução, deverá ser ministrado treinamento para a equipe da contratante sobre os recursos que a solução Wireless poderá disponibilizar, enfatizando as topologias de rede, funcionalidades e de recursos de segurança que poderiam ser implementados.
2.3.6.3. Do Treinamento
2.3.6.3.1. O treinamento deverá ter a duração mínima de 20 (vinte) horas;
2.3.6.3.2. O treinamento será ministrado para uma turma de até 12 (doze) alunos, em turnos de 04 (quatro) horas por dia em 05 (cinco) dias úteis;
2.3.6.3.3. O treinamento poderá ser feito de forma remota em plataforma a ser definida pela contratada;
2.3.6.3.4. O conteúdo a ser abordado no treinamento deverá ser elaborado pela contratada e necessitará de aprovação pela equipe da contratante;

2.3.6.3.5. A data para realização do treinamento deverá ser estabelecida em conjunto pela contratada e contratante;
2.3.6.3.6. Ao final do treinamento deverá ser emitido certificado de participação para cada aluno;
2.3.6.4. Do Serviço de Instalação e Configuração
2.3.6.4.1. Do Planejamento
2.3.6.4.1.1. O planejamento das ações a serem executadas para e instalação e configuração dos serviços deverá ser feito em no máximo 12 horas e será realizado em conjunto pelas equipes da contratada e contratante, equipes que deverão ser montadas em até 72 horas após a assinatura do contrato.
2.3.6.4.1.2. O planejamento deverá abordar os aspectos relacionados à topologia de rede, funcionalidades e de recursos de segurança a serem implementados.
2.3.6.4.1.3. A realização dos serviços deve ser planejada de acordo com disponibilidade de ambas as partes, em prazo máximo de 30 dias após a entrega definitiva dos bens ou oficialização da ordem de empenho. O planejamento anterior ao serviço pode ser realizado remotamente através de webconferência ou videoconferência;
2.3.6.4.1.4. O planejamento dos serviços de instalação deve resultar em um documento tipo SOW (em tradução livre, escopo de trabalho). Neste documento devem conter a relação de produtos; descrição e quantidades de equipamentos e serviços; descrição da infraestrutura atual e desejada; detalhamento dos serviços que serão executados; premissas do projeto; local, horários e condições de execução dos serviços; pontos de contato da contratante e contratada; cronograma faseado do projeto, divido em etapas, com responsáveis e data e início e fim (se aplicável); relação da documentação a ser entregue ao final da execução dos serviços; responsabilidade da contratante e contratada; plano de gerenciamento de mudanças; itens excluídos no projeto; e termo de aceite. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes;
2.3.6.4.2. Da Instalação e Configuração
2.3.6.4.2.1. Descrição dos serviços:
2.3.6.4.2.1.1. Configuração da autenticação dos usuários wireless por meio da base de usuários do servidor de diretório da contratante, utilizando o protocolo IEEE 802.1x, de modo que o acesso do usuário seja liberado pela solução apenas após sua autenticação;
2.3.6.4.2.1.2. Configuração para permitir autenticação Web para estações de trabalho sem cliente 802.1x instalado;
2.3.6.4.2.1.3. Configuração para permitir autenticação pelo MAC Address, para dispositivos sem cliente 802.1x e sem browser;
2.3.6.4.2.1.4. Configuração das assinaturas de wIDS/wIPS;
2.3.6.4.2.1.5. Configuração de políticas de bloqueio de rogue APs;
2.3.6.4.2.1.6. Configuração para classificação/detecção de interferências WiFi e não-WiFi;
2.3.6.4.2.1.7. Configurar o controle de aplicações permitindo ao administrador filtrá-las para que seja obedecida a política de segurança já em operação na contratante;
2.3.6.4.2.1.8. Configuração de um portal de autenticação web para os usuários visitantes, com as seguintes funcionalidades:
2.3.6.4.2.1.9. Funcionar de forma criptografada com o uso de certificados (SSL);
2.3.6.4.2.1.9.1. Criar um certificado auto-assinado;
2.3.6.4.2.1.9.2. Customizar com logotipo e políticas de acesso;
2.3.6.4.2.1.9.3. Check-box para aceite com as políticas de acesso da rede;
2.3.6.4.2.1.9.4. Configurar regras de acesso que permitem acessos a serviços específicos antes da autenticação, por exemplo, DHCP;
2.3.6.4.3. A contratada deve ainda, após a instalação e configuração, monitorar a solução pelo prazo mínimo de 8 (oito) horas corridas, sendo possível o troubleshooting em caso de problemas ou não conformidades na operação. Durante este período deve ser observado e realizado também os

ajustes e configurações que porventura não estarão de acordo com a operação desejada por este órgão;

2.3.6.4.4. Ao final da instalação e monitoramento, deverá ser realizado repasse de conhecimento de toda a solução por um período de 4 (quatro) horas corridas;

2.3.6.4.5. Os serviços devem ser executados de segunda a sexta-feira, das 8 às 18 horas, nas unidades da contratante;

2.3.6.4.6. Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados no projeto (as-built), etapas de execução e toda informação pertinente a posterior continuidade e manutenção da solução instalada;

2.4. Possíveis Soluções de Tecnologia da Informação e Comunicação (Art 14, II)

Não se aplica, tendo em vista que a aquisição visa apenas a recuperação e expansão da rede sem fio já instalada, não havendo mudança e nem implantação de nova de tecnologia.

2.5. Comparação entre os custos totais das Soluções de Tecnologia da Informação e Comunicação (Art 14, III)

Conforme item 2.4

2.6. Solução de Tecnologia da Informação e Comunicação escolhida (Art 14, IV)

2.6.1. Descrição

Pontos de Acesso WIFI nos modelos Cisco Aironet 9105, Cisco Aironet 9115 e Cisco Aironet 1562i, Controladora Wireless Virtual – C9800-CI, Licença para Ponto de Acesso - DNA Essentials além de Serviço de Instalação, Configuração e Treinamento na Solução Wireless.

2.6.2 Justificativa

Pela necessidade de utilização de equipamentos específicos para a recuperação e ampliação das redes sem fio já instaladas, pois precisa ser compatível com o fabricante e o modelo já adquirido anteriormente.

2.7. Benefícios Esperados

Aumento da performance e segurança das redes já instaladas e ampliação do número de prédios com disponibilidade de rede sem fio (WIFI), permitindo com isso a manutenção e ampliação da oferta de serviços de TI.

2.8. Necessidades de adequação do ambiente do órgão

Não haverá necessidade de adequação de ambiente.

2.9. Orçamento estimado

Foram enviadas solicitações de cotação para as empresas CI STORE, MultiNetwork Brasil LTDA, Teltec Solutions LTDA, Muld Comércio e Serviços de Informática Ltda, Need TI Hardware e Meganet Comércio e Serviços que são fornecedoras autorizadas pelo fabricante dos equipamentos no Brasil.

Somente as empresas Teltec Solutions LTDA, Muld Comércio e Serviços de Informática Ltda e Meganet Comércio e Serviços enviaram propostas.

A Tabela abaixo apresenta informações resumidas das propostas:

ITEM	Meganet Comércio e Serviços	Muld Informática Ltda	Teltec Solutions LTDA	Preço Médio	Quantidade	Total por Item
Ponto de acesso interno - Aironet 9105	R$ 7.000,00	R$ 8.400,00	R$ 6.850,00	R$ 7.416,66	400	R$ 2.966.664,00
Ponto de acesso interno - Aironet 9115	R$ 11.560,00	R$ 9.980,00	R$ 10.800,00	R$ 10.780,00	100	R$ 1.078.000,00
Ponto de acesso externo - Aironet 1562i	R$ 12.900,00	R$ 14.900,00	R$ 13.000,00	R$ 13.600,00	10	R$ 136.000,00
Controladora Wireless Virtual – C9800-CI	R$ 7.000,00	R$ 8.050,00	R$ 5.000,00	R$ 6.683,33	1	R$ 6.683,33
Licença para Ponto de Acesso - DNA Essentials	R$ 1.310,00	R$ 2.000,00	R$ 1.310,00	R$ 1.540,00	82	R$ 126.280,00
Serviço de Instalação, Configuração e Treinamento na Solução Wireless	R$ 30.000,00	R$ 40.000,00	R$ 35.000,00	R$ 35.000,00	1	R$ 35.000,00
Valor Total Geral =						**R$ 4.348.627,33**

O preço médio do Ponto de acesso interno - Aironet 9105 é de **R$ 7.416,66 (Sete mil, quatrocentos e dezesseis reais e sessenta e seis centavos)**, o preço médio do Ponto de acesso interno - Aironet 9115 é de **R$ 10.780,00 (Dez mil, setecentos e oitenta reais)**, o preço médio do Ponto de acesso externo - Aironet 1562i é de **R$ 13.600,00 (Treze mil e seiscentos reais)**, o preço médio da Controladora Wireless Virtual – C9800-CI é de **R$ 6.683,33 (Seis mil, seiscentos e oitenta e três reais e trinta e três centavos)**, o preço médio da Licença para Ponto de Acesso - DNA Essentials é de **R$ 1.540,00 (Um mil, quinhentos e quarenta reais)** e o preço médio do Serviço de Instalação, Configuração e Treinamento na Solução Wireless é de **R$ 35.000,00 (Trinta e cinco mil reais).**

O custo total estimado é de **R$ 4.348.627,336 (Quatro milhões, trezentos e quarenta e oito mil, seiscentos e vinte e sete reais e trinta e três centavos)**.

3. SUSTENTAÇÃO DO CONTRATO (Art 15)

O plano de sustentação tem por finalidade garantir a continuidade da operação da Solução de TIC após o término do contrato, tanto se o término ocorrer de forma prevista ou imprevista.

Considerando a natureza e simplicidade da presente contratação que é a aquisição de dispositivos em uma única parcela e que as obrigações da contratada se encerrará com o fornecimento do objeto, não caracterizando prestação de serviços que na sua falta deverá ser absorvida por recursos próprios do Órgão, não cabe elaboração plano de sustentação.

3.1. Recursos necessários à continuidade do objeto contratado (Art 15, I)

Não se aplica, conforme item 3.

3.2. Continuidade do fornecimento da Solução de TIC em eventual interrupção contratual (Art 15, II)

Não se aplica, conforme item 3.

3.3. Das atividades de transição contratual e de encerramento do contrato (Art 15, III)

Não se aplica, conforme item 3.

3.4. Regras para estratégia de independência do órgão com relação à empresa contratada (Art 15, IV)

Não se aplica, conforme item 3.

4. ESTRATÉGIA PARA CONTRATAÇÃO (Art 16)

4.1. Natureza do Objeto (Art 16, I)

O objeto possui características comuns e usuais encontradas no mercado de TIC, cujos padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital.

Destarte, essa equipe de planejamento compreende que o serviço almejado se enquadra na categoria de SERVIÇO NÃO CONTINUADO, pois trata-se de aquisição de bens em parcela única.

4.2. Parcelamento do Objeto (Art 16, II)

- Por se tratar da aquisição de bens com tecnologias que necessitam ser compatíveis entre si, a aquisição em um único Lote é a forma mais adequada de parcelamento. O objeto deverá ser fornecido por uma única empresa e em uma única parcela.

4.3. Adjudicação e Fornecimento (Art 16, III)

- Será adjudicado em lote único para o fornecedor que ofertar o menor preço.

4.4. Modalidade e tipo de licitação (Art 16, IV)

- Será utilizada a modalidade de Pregão Eletrônico, tipo menor preço global.

4.5. Classificação Orçamentária e Fonte de Recursos (Art 16, V)

- Definição a ser feita pela Diretoria Financeira.

4.6. Vigência / Garantia da Aquisição de bens (Art. 16, VI)

- Sugere-se que a vigência do contrato decorrente do certame seja de 12 (doze) meses.

4.7. Equipe de apoio a Contratação e Fiscalização do Contrato (Art 16, VII)

Servidor 1		
Nome	**Matrícula**	**Telefone**
Leonardo Araújo Sousa	129502	98 3194 5887

Servidor 2		
Nome	**Matrícula**	**Telefone**
José Eduardo Carvalho Thomaz	129437	98 3194 5870

4.8. Equipe de Gestão do Contrato (Art 16, VIII)

A gestão do referido contrato ficará sob a responsabilidade da Diretoria de Informática e Automação, conforme Resolução GP 212018.

5. ANÁLISE DE RISCOS (Art. 17)

5.1. Identificação dos Riscos

Nº	Risco	Probabilidade	Severidade	Potencial	Fase
01	Licitação Deserta	1	3	3	Contratação
02	Cotação incompatível com o objeto ou desatualizada	2	3	6	Contratação
03	Recursos Administrativos durante o Pregão	1	2	3	Contratação
04	Pedidos de Impugnação de Edital	2	2	4	Contratação
05	Objeto não atende as necessidades	1	3	3	Contratação
06	Atraso de Fornecimento	1	3	3	Execução
07	Serviços de garantia inoperante	1	3	3	Execução
08	Defeito de fabricação do objeto	2	3	6	Execução

5.2 Planos de ação

Risco	Ação Preventiva	Ação de Contingência	Responsável
01	Elaborar especificações técnicas compatíveis com produtos existentes no mercado	Realizar replanejamento da contratação.	Equipe de Planejamento da Contratação
02	Apoiar Setor de Cotação na pesquisa de preços	Realizar replanejamento da contratação.	Equipe de apoio a contratação
03	Redigir especificações técnicas de forma clara e objetiva	Responder recursos Administrativos	Equipe de Planejamento da Contratação e Equipe de Apoio a Contratação
04	Redigir especificações técnicas de forma clara e objetiva	Responder recursos Administrativos	Equipe de Planejamento da Contratação e Equipe de Apoio a Contratação
05	Realizar testes de amostras antes da homologação das propostas classificadas	Recusar objeto	Equipe de Apoio a Contratação
06	Manter canal de relacionamento com o fornecedor informando a tramitação do processo a fim de prepará-lo para fabricação e fornecimento dos produtos.	Aplicar sanções contratuais	Equipes de Fiscalização e Gestão do Contrato
07	Monitorar riscos	Aplicar sanções contratuais	Equipes de Fiscalização e Gestão do Contrato
08	Realizar testes de conformidade dos produtos antes da aceitação.	Recusar Fornecimento	Equipes de Fiscalização e Gestão do Contrato